Capítulo 2

Números naturales y números enteros

Empezamos aquí a estudiar los números naturales. Todos sabemos que al hablar de los números naturales nos estamos refiriendo a los números $0, 1, 2, \cdots$. Sin embargo, para un estudio de algunas propiedades de los números naturales esta definición de números naturales es totalmente insuficiente. Necesitamos fijar una base como punto de arranque, a partir de la cual iremos desarrollando la teoría.

La primera cuestión que nos planteamos es dónde situar el punto de partida. Las posibilidades son varias. Por ejemplo, podemos empezar postulando la existencia de un conjunto (los números naturales) que satisface una serie de axiomas (los axiomas de Peano). A partir de estos axiomas podemos definir las operaciones básicas que todos conocemos (suma y producto) y el orden.

También es posible situar el punto de arranque en la teoría de conjuntos, y en el marco de esta teoría construir un conjunto ($\mathbb{N}$) del cual se demuestra que satisface los axiomas de Peano. En este caso, los axiomas de Peano son una consecuencia de la construcción hecha de $\mathbb{N}$, mientras que en el caso anterior estos axiomas constituyen el principio de la teoría. Una vez demostrados los axioms de Peano, se enlaza con el caso anterior.

Estos planteamientos, sin embargo, no nos interesan en este momento. Nosotros supondremos que tenemos un conjunto, representado por $\mathbb{N}$, cuyos elementos son los números naturales, y que en este conjunto tenemos definidas dos operaciones (suma y producto), de las que conocemos sus propiedades básicas. Tenemos definido también un orden de los números naturales, y sabemos que los números naturales satisfacen el axioma de inducción. En la sección siguiente recordaremos todas estas propiedades y axiomas.

También supondremos la existencia de los números enteros ($\mathbb{Z}$), los números racionales ($\mathbb{Q}$), los números reales ($\mathbb{R}$) y los números complejos ($\mathbb{C}$) con su estructura algebraica y de orden (salvo en $\mathbb{C}$).

2.1. Representación de los números naturales. Sistemas de numeración.

2.1.1. El conjunto de los números naturales.

Como hemos dicho, comenzamos suponiendo que tenemos un conjunto $\mathbb{N}$. Los elementos de este conjunto se llaman *números naturales.*

Dados dos números naturales, m y n, hay definidos dos nuevos números naturales, llamados respectivamente suma y producto de m y n, y representados mediante $m+n$ y $m \cdot n$ (o simplemente mn). Estas operaciones satisfacen las siguientes propiedades:

i) Para cualesquiera $m, n, p \in \mathbb{N}$, $(m+n)+p = m+(n+p)$ (es decir, la suma es asociativa).

ii) Para cualesquiera $m, n \in \mathbb{N}$, $m+n = n+m$ (es decir, la suma es conmutativa).

iii) Existe en $\mathbb{N}$ un elemento, representado por 0 tal que para cada $m \in \mathbb{N}$ se tiene que $m+0 = m$ (existencia de elemento neutro para la suma).

iv) Si $m+n = m+p$ entonces $n = p$ (Propiedad cancelativa).

v) Para cualesquiera $m, n, p \in \mathbb{N}$, $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ (es decir, el producto es asociativo).

vi) Para cualesquiera $m, n \in \mathbb{N}$, $m \cdot n = n \cdot m$ (es decir, el producto es conmutativo).

vii) Existe en $\mathbb{N}$ un elemento, representado por 1 tal que para cada $m \in \mathbb{N}$ se tiene que $m \cdot 1 = m$ (existencia de elemento neutro para el producto).

viii) Si $m \cdot n = m \cdot p$ y $m \neq 0$ entonces $n = p$.

ix) Para cualesquiera $m, n, p \in \mathbb{N}$, $m \cdot (n + p) = m \cdot n + m \cdot p$ (la suma es distributiva respecto al producto).

También en $\mathbb{N}$ hay definida una relación como sigue:

$$m \leq n \text{ si existe } p \in \mathbb{N} \text{ tal que } m + p = n$$

que satisface las siguientes propiedades:

x) $m \leq m$ para todo $m \in \mathbb{N}$.

xi) Si $m \leq n$ y $n \leq m$ entonces $m = n$.

xii) Si $m \leq n$ y $n \leq p$ entonces $m \leq p$,

xiii) Para cualesquiera $m, n \in \mathbb{N}$, $m \leq n$ ó $n \leq m$.

xiv) $m \leq n$ implica que $m + p \leq n + p$ para todo $p \in \mathbb{N}$.

xv) $m + p \leq n + p$ implica que $m \leq n$.

xvi) $m \leq n$ implica que $m \cdot p \leq n \cdot p$.

xvii) Si $m \cdot p \leq n \cdot p$ y $p \neq 0$ entonces $m \leq n$.

Todo lo dicho anteriormente es igualmente válido para otros conjuntos, como $\mathbb{Q}^+$, $\mathbb{R}^+$, etc. Lo que distingue a $\mathbb{N}$ de estos conjuntos es el *Principio de inducción.*

Principio de inducción:

Si A es un subconjunto de $\mathbb{N}$ tal que:

$0 \in A$

Si $n \in A$ entonces $n + 1 \in A$

Entonces $A = \mathbb{N}$.

Intuitivamente, nos dice que los números naturales podemos recorrerlos *de uno en uno,* y no nos dejamos ninguno en medio, es decir, cualquier número natural puede ser obtenido a partir del cero sin más que sumar uno las veces que sean necesarias. Si lo pensamos, para los conjuntos $\mathbb{Q}^+$ o $\mathbb{R}^+$ no se cumple esta propiedad, pues procediendo así siempre nos dejamos números "en medio".

El principio de inducción está en la base de la recursividad, y por tanto en la de muchas demostraciones en las que intervienen los números naturales. Nosotros, sin embargo, no vamos a profundizar en este principio, ni en las demostraciones por inducción.

Una consecuencia de este principio, junto con las propiedades anteriores es que si $m < n$ entonces $m + 1 \leq n$.

Recordemos también que dados dos números naturales m y n, tenemos definido el número m^n (salvo cuando $m = n = 0$), que representa el producto de m consigo mismo n veces. Es decir, $m^1 = m$, $m^2 = m \cdot m$, $m^3 = m \cdot m \cdot m$, etc. Sabemos que a m^0 se le asigna el valor 1, y que esta operación satisface las siguientes propiedades:

xviii) Para cualesquiera $m, n, p \in \mathbb{N}$, con $m \neq 0$, $m^{n+p} = m^n \cdot m^p$.

xix) Para cualesquiera $m, n, p \in \mathbb{N}$, con $m \neq 0$, $(m^n)^p = m^{n \cdot p}$.

xx) Para cualesquiera $m, n, p \in \mathbb{N}$, con $m, n \neq 0$, $(m \cdot n)^p = m^p \cdot n^p$.

Una consecuencia del principio de inducción es el siguiente teorema:

Teorema 2.1.1. *[Principio de buena ordenación] Sea B un subconjunto no vacío de $\mathbb{N}$. Entonces B tiene mínimo.*

Demostración: Tomamos A el conjunto de las cotas inferiores de B. Es claro que $0 \in A$ y que $A \neq \mathbb{N}$ (ya que si $m \in B$ entonces $m + 1 \notin A$). Ahora bien. Si el enunciado $n \in A \Longrightarrow n + 1 \in A$ fuera cierto, tendríamos que $A = \mathbb{N}$, lo cual no es posible. Por tanto, debe ser falso, lo que nos dice que tiene que existir un elemento m_0 tal que $m_0 \in A$ pero $m_0 + 1 \notin A$.

Entonces, este elemento es el mínimo de B. Para esto, deben ocurrir dos cosas: que sea cota inferior (lo cual es cierto, pues es elemento de A) y que pertenezca a B. Veamos esto último.

Si $m_0 \notin B$ significa que $m_0 < n$ para cualquier $n \in B$, luego $m_0 + 1 \leq n$ para cualquier $n \in B$, lo que implicaría que $m_0 + 1$ es cota inferior de B y por consiguiente pertenecería a A. ■

Como consecuencia de esto, tenemos:

Corolario 2.1.1. *No existen sucesiones en $\mathbb{N}$ infinitas y estrictamente decrecientes.*

Demostración: Si $x_0, x_1, \cdots, x_m, \cdots$ fuera una tal sucesión, entonces el conjunto $\{x_n : n \in \mathbb{N}\}$ tendría mínimo, que tendría que corresponder con algún término de la sucesión, digamos x_k. Pero en tal caso, $x_{k+1} < x_k$ por ser la sucesión estrictamente decreciente, lo que nos dice que dicho término no puede ser el mínimo. ■

Tras esta introducción, nos adentramos ya en materia. Comenzamos por un resultado de todos conocido.

Teorema 2.1.2. *[Algoritmo de la división] Sean $a, b \in \mathbb{N}$, con $b \neq 0$. Entonces existen únicos elementos $c, r \in \mathbb{N}$ tales que:*

- $a = bc + r$.
- $r < b$.

Obviamente, lo único que estamos haciendo es la división usual de a entre b.

Los números c y r se llaman respectivamente cociente y resto de la división de a entre b.

La demostración de este teorema se haría usando el principio de inducción. Pero nosotros daremos por cierto este resultado.

Definición 32. *Sean $a, b \in \mathbb{N}$. Se definen los números naturales a mód b y a div b como los únicos números naturales que satisfacen que*

$$a = b \cdot (a \ div \ b) + (a \ mód \ b); \qquad a \ mód \ b < b$$

Es decir, a mód b es el resto que resulta de dividir a entre b y a div b es el cociente de dividir a entre b.

Ejemplo 2.1.1. *Se tiene que 13 mód $3 = 1$ y 13 div $3 = 4$, pues $13 = 3 \cdot 4 + 1$.*

Notemos que si $a \neq 0$ y $b \geq 2$ entonces a div $b < a$ (¿por qué?).

2.1.2. Sistemas de numeración.

Sabemos que el conjunto de los números naturales es infinito. Sin embargo, para representar un número natural, empleamos únicamente los símbolos 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9. Con estos símbolos, llamados dígitos, combinados de manera adecuada podemos representar todos los números naturales. Los números 0 y 1 representan los elementos neutros para la suma y el producto. El resto de los números, representados por estos dígitos puede obtenerse fácilmente mediante $2 = 1 + 1$, $3 = 2 + 1$, y así sucesivamente hasta $9 = 8 + 1$. El número siguiente, es decir $9 + 1$ es representado, como todos sabemos como 10.

En una representación de un número natural, el valor de cada uno de estos dígitos depende de la posición que ocupe. Así, en el número 1343 no representa lo mismo el dígito 3 situado a la derecha que el dígito 3 situado entre los dígitos 1 y 4. Analizando algo más el valor de cada uno de los dígitos, vemos que el valor del 1 que se encuentra a la izquierda es 10^3, el valor del 3 que se encuentra inmediatamente a la derecha es $3 \cdot 10^2$, el valor del 4 es $4 \cdot 10$, mientras que el valor del 3 situado a la derecha es 3. El número representado mediante 1343 es entonces la suma de todos estos resultados, es decir, $1343 = 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 3$.

El origen de la elección de 10 como base de la representación de los números naturales parece ser que se encuentra en el número de dedos que tenemos en las manos. Nos planteamos ahora qué ocurriría si en lugar de elegir como base a 10 eligieramos cualquier otro número b. La respuesta viene en el siguiente teorema.

Teorema 2.1.3. *Sean $a, b \in \mathbb{N}$ con $a \neq 0$ y $b \geq 2$. Entonces existen únicos $m \in \mathbb{N}$ y $a_0, a_1 \cdots, a_m \in \mathbb{N}$ tales que:*

- $a_m \neq 0$.
- $a = \sum_{k=0}^{m} a_k b^k = a_m b^m + \cdots + a_1 b + a_0$
- $a_i < b$.

Demostración:

Probemos en primer lugar la existencia de estos números.

En el caso de que $a < b$ entonces podemos tomar $m = 0$, $a_0 = a$.

Supongamos entonces que $a \geq b$. Dividimos a entre b, y obtenemos un cociente que llamaremos c_1 y un resto que llamaremos a_0. En tal caso, tenemos que $a = b \cdot c_1 + a_0$.

Es claro que $1 \leq c_1 < a$. Si $c_1 < b$ entonces tomamos $m = 1$, $a_1 = c_1$, y ya tendríamos la existencia de m y los coeficientes a_i. Si $c_1 \geq b$, entonces dividimos c_1 entre b, y obtenemos un cociente c_2 y un resto a_1, es decir, $c_1 = b \cdot c_2 + a_1$, luego

$$a = b \cdot c_1 + a_0 = b \cdot (b \cdot c_2 + a_1) = c_2 \cdot b^2 + a_1 \cdot b + a_0$$

Repetimos con c_2 lo mismo que con c_1, y así tenemos una sucesión decreciente de números naturales $a > c_1 > c_2 > \cdots$ Esta sucesión no puede ser infinita (corolario 2.1.1). Si c_k es su último término, entonces $c_k < b$. En tal caso, tomamos $m = k$ y $a_k = c_k$, en cuyo caso:

$$a = b \cdot c_1 + a_0 = c_2 b^2 + a_1 b + a_0 = c_3 b^3 + a_2 b^2 + a_1 b + a_0 = \cdots = c_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

como queríamos.

La demostración de la unicidad se deja como ejercicio.

■

Ejemplo 2.1.2. *Tomemos, por ejemplo, $b = 5$ y el número $a = 446$. Vamos a hallar los distintos números que nos dice el teorema.*

Puesto que $446 \geq 5$, realizamos la división $446 = 5 \cdot 89 + 1$. En tal caso, $a_0 = 1$ y $c_1 = 89$.

Al ser $c_1 \geq 5$ repetimos el proceso. $89 = 5 \cdot 17 + 4$. Esto nos da $a_1 = 4$ y $c_2 = 17$. Entonces,

$$446 = 5 \cdot 89 + 1 = 5 \cdot (5 \cdot 17 + 4) + 1 = 5^2 \cdot 17 + 5 \cdot 4 + 1 = 17 \cdot 5^2 + 4 \cdot 5 + 1$$

Continuamos, pues $c_2 \geq 5$. Ahora tenemos $17 = 5 \cdot 3 + 2$. Por tanto, $a_2 = 2$ y $c_3 = 3$. Sustituimos, y nos queda:

$$446 = 17 \cdot 5^2 + 4 \cdot 5 + 1 = (3 \cdot 5 + 2) \cdot 5^2 + 4 \cdot 5 + 1 = 3 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 1$$

Y ya tenemos que el cociente, c_3, es menor que la base. Por tanto, $m = 3$ y $a_3 = c_3 = 3$.

En resumen, tenemos que $m = 3$ *y los coeficientes son* $a_0 = 1$, $a_1 = 4$, $a_2 = 2$ *y* $a_3 = 3$.

La demostración anterior nos proporciona un algoritmo recursivo para calcular estos coeficientes.

Algoritmo BASE(a, b)

Entrada: $a, b \in \mathbb{N}$; $a \geq 1, b \geq 2$.

Salida: $m, a_0, a_1, \cdots, a_m$
$m \in \mathbb{N}$
$a_0, a_1, \cdots, a_m \in \mathbb{N}$
$0 \leq a_i < b$
$a_m \neq 0$
$a = a_m \cdot b^m + a_{m-1} \cdot b^{m-1} + \cdots + a_1 \cdot b + a_0$

$m := 0$
Mientras $a \geq b$
$a_m := a$ mód b
$a := a$ div b
$m := m + 1$
$a_m := a$
Devuelve $m, a_0, a_1, \cdots, a_m$

Ejemplo 2.1.3.
Vamos a repetir el ejemplo anterior, es decir, $a = 446$ *y* $b = 5$. *Los resultados los vamos a ir ordenando en una tabla.*
Los valores iniciales son $b = 5$ *(que no varía),* $a = 446$ *y* $m = 0$.

b	5
a	446
m	0
a_m	

Puesto que $a \geq b$ *entramos en el bucle, lo que nos da* $a_m = a_0 = 446$ *mód* $5 = 1$, $a = 446$ *div* $5 = 89$ *y* $m = 1$.

b	5	
a	446	89
m	0	1
a_m	1	

Ahora también $a = 89$ *es mayor que* $b = 5$, *por lo que volvemos a entrar en el bucle.* $a_1 = 89$ *mód* $5 = 4$, $a = 89$ *div* $5 = 17$ *y* $m = 2$.

b	5		
a	446	89	17
m	0	1	2
a_m	1	4	

Se tiene que $17 \geq 5$. *Entonces* $a_2 = 17$ *mód* $5 = 2$, $a = 17$ *div* $5 = 3$ *y* $m = 3$.

b	5			
a	446	89	17	3
m	0	1	2	3
a_m	1	4	2	

Y ahora, como $a < b$, *hacemos* $a_3 = 3$

b	5			
a	446	89	17	3
m	0	1	2	3
a_m	1	4	2	3

y terminamos: $m = 3$ *y* $a_0 = 1$, $a_1 = 4$, $a_2 = 2$ *y* $a_3 = 3$, *de donde* $446 = 3 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 1$.

Definición 33. *Sean* $a, b \in \mathbb{N}$ *con* $b \geq 2$. *Elegimos* b *símbolos que se corresponden con los números desde* 0 *hasta* $b-1$, *e identificamos estos números con sus símbolos. Supongamos que* $a = a_m b^m + \cdots + a_1 b + a_0$ *con* $a_i < b$. *Diremos entonces que* $a_m a_{m-1} \cdots a_1 a_0$ *es una representación del número* a *en base* b, *y escribiremos*

$$a = (a_m a_{m-1} \cdots a_1 a_0)_b$$

Observaciones:

1. Cada uno de los símbolos que aparecen en la representación de un número se denomina cifra.

2. Si $a = (a_m \cdots a_1 a_0)_b$, podemos añadir ceros a la izquierda y obtenemos también una representación de a. Normalmente, elegiremos como representación de a aquella para la que la cifra de la izquierda sea distinta de cero (si el número a es distinto de cero).

3. Si $a = (a_m \cdots a_1 a_0)_b$ y $a_m \neq 0$, diremos que el número a tiene $m+1$ cifras en base b.

4. A la hora de especificar la base lo haremos en base decimal. Si la expresáramos en base b nos quedaría siempre 10.

5. Cuando no se especifique la base en que está expresado un número supondremos que está en base diez, salvo que el contexto deje suficientemente claro la base en que estamos trabajando.

6. Cuando trabajamos en base diez, los símbolos empleados son, como todos sabemos, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Si trabajamos en una base b menor que diez, emplearemos los símbolos anteriores hasta $b-1$. Por ejemplo, en base 2 se emplean $0, 1$. Cuando la base sea mayor que 10, como símbolos adicionales se suelen emplear las letras del alfabeto (siempre y cuando la base no sea muy grande). Es muy frecuente trabajar en base dieciseis, en cuyo caso, los símbolos empleados son 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Ejemplo 2.1.4.

1. *Si queremos expresar el número* 446 *en base* 5, *necesitamos una expresión de este número en función de potencias de* 5. *Sabemos que* $446 = 3 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 1$, *luego*

$$446 = (3241)_5$$

2. *Vamos a expresar el número* $(23143)_6$ *en base* 8. *Para esto, podemos pasarlo a base decimal y después pasarlo a base* 8.

$$(23143)_6 = 2 \cdot 6^4 + 3 \cdot 6^3 + 6^2 + 4 \cdot 6 + 3 = 2 \cdot 1296 + 3 \cdot 216 + 36 + 4 \cdot 6 + 3 = 3303$$

$3303 = 8 \cdot 412 + 7 \quad 412 = 8 \cdot 51 + 4 \quad 51 = 8 \cdot 6 + 3$

Por tanto tenemos que $(23143)_6 = 3303 = (6347)_8$

3. *Vamos ahora a expresar el número* $(10101111011000001010100)_2$ *en base* 8 *y en base* 16. *En primer lugar lo pasamos a base decimal.*

$(10101111011000001010100)_2 = 2^{22} + 2^{20} + 2^{18} + 2^{17} + 2^{16} + 2^{15} + 2^{13} + 2^{12} + 2^6 + 2^4 + 2^2 = 5746772$

Nos apoyamos ahora en el algoritmo BASE

b	8							
a	5746772	718346	89793	11224	1403	175	21	2
m	0	1	2	3	4	5	6	7
a_m	4	2	1	0	3	7	5	2

y de aquí deducimos que $(10101111011000001010100)_2 = (25730124)_8$

Para expresar el número en base 16*, volvemos a hacer uso del algoritmo BASE para los valores* $a = 5746772$ *y* $b = 16$*.*

b	16					
a	5746772	359173	22448	1403	87	5
m	0	1	2	3	4	5
a_m	4	5	0	11	7	5

luego $(10101111011000001010100)_2 = (57B054)_{16}$ *(donde, como dijimos antes, hemos empleado los símbolos* $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$*).*

Ahora bien, dado que $8 = 2^3$*, podíamos haber procedido como sigue:*

$$\begin{aligned}(10101111011000001010100)_2 &= 2^{22} + 2^{20} + 2^{18} + 2^{17} + 2^{16} + 2^{15} + 2^{13} + 2^{12} + 2^6 + 2^4 + 2^2 \\ &= 2 \cdot 2^{21} + (2^2 + 1)2^{18} + (2^2 + 2 + 1)2^{15} + (2 + 1)2^{12} + 2^6 + 2 \cdot 2^3 + 2^2 \\ &= 2 \cdot 8^7 + 5 \cdot 8^6 + 7 \cdot 8^5 + 3 \cdot 8^4 + 8^2 + 2 \cdot 8 + 4\end{aligned}$$

y como $16 = 2^4$*, podíamos haberlo hecho de forma análoga:*

$$\begin{aligned}(10101111011000001010100)_2 &= 2^{22} + 2^{20} + 2^{18} + 2^{17} + 2^{16} + 2^{15} + 2^{13} + 2^{12} + 2^6 + 2^4 + 2^2 \\ &= (2^2 + 1)2^{20} + (2^2 + 2 + 1)2^{16} + (2^3 + 2 + 1)2^{12} + (2^2 + 1)2^4 + 2^2 \\ &= 5 \cdot 16^5 + 7 \cdot 16^4 + 11 \cdot 16^3 + 5 \cdot 16 + 4\end{aligned}$$

y de aquí es fácil obtener la representación del número dado en base 8 *y en base* 16*.*

Podemos apreciar como para pasar de base 2 *a base* $8 = 2^3$ *podemos agrupar las cifras del número en base* 2 *de tres en tres (empezando por la derecha). Cada uno de estos tres grupos da lugar a una cifra en base* 8*. De la misma forma, cada* 4 *cifras de un número en base* 2 *da lugar a una cifra del mismo número en base* 16*.*

$$\underbrace{1}_{2}\underbrace{0\,1}_{5}\underbrace{0\,1\,1}_{7}\underbrace{1\,0\,1\,1}_{3}\underbrace{0\,0\,0\,0}_{0}\underbrace{0\,1\,0\,1}_{1}\underbrace{0\,1\,0\,0}_{2}\underbrace{}_{4} \qquad \underbrace{101}_{5}\underbrace{0111}_{7}\underbrace{1011}_{B}\underbrace{0000}_{0}\underbrace{0101}_{5}\underbrace{0100}_{4}$$

En general, para pasar un número de base b *a base* b^k *basta con agrupar las cifras del número escrito en base* b *en grupos de* k *cifras, empezando por la derecha. Cada uno de estos grupos determina una cifra en base* b^k*.*

Recíprocamente, para pasar un número de base b^k *a base* b *es suficiente expresar cada cifra del número en base* b *(completando con ceros a la izquierda para que nos de* k *cifras).*

4. *Vamos a encontrar una base* b *donde se de la igualdad* $21 \cdot 23 = 1033$*.*

   Obviamente, b *debe ser mayor o igual que* 4*, pues en otro caso no podríamos tener el dígito* 3*.*

   Al estar escritos los números en base b *lo que tenemos es la igualdad*

   $$(2b + 1)(2b + 3) = b^3 + 3b + 3$$

   Operando nos queda $b^3 - 4b^2 - 5b = 0$*, que podemos comprobar que tiene tres raíces, que son* $b = -1$*,* $b = 0$ *y* $b = 5$*. La solución es por tanto* $b = 5$*.*

Los algoritmos que conocemos para sumar, restar, multiplicar o dividir números escritos en base 10 son válidos ahora para realizar estas operaciones para números escritos en una base b cualquiera.

Así, por ejemplo, para la suma, si $m, n \in \mathbb{N}$; $m = (m_k m_{k-1} \cdots m_1 m_0)_b$ y $n = (n_k n_{k-1} \cdots n_1 n_0)_b$ (hemos supuesto que los dos números tienen igual número de cifras. De no ser así, añadimos "ceros" al que tenga menos), entonces $m + n = (p_{k+1} p_k \cdots p_1 p_0)_b$ donde:

- $p_0 = (m_0 + n_0)$ *mód* b

- $p_{i+1} = (m_{i+1} + n_{i+1} + a_i)$ *mód* b, donde $a_i = (m_i + n_i + a_{i-1})$ *div* b (hemos tomado $a_{-1} = 0$).

Es fácil comprobar que el número $(p_{k+1}p_k \cdots p_1p_0)_b$ aquí descrito corresponde con la suma de m y n (hágase).

Este algoritmo puede extenderse sin difucultad a la suma de tres o más números. Para el caso que hemos detallado de dos números, a_i únicamente puede tomar los valores 0 y 1.

En el caso $b = 10$, lo que hemos dicho es simplemente el método tradicional que usamos para sumar dos (o más) números.

Ejemplo 2.1.5. *Sean* $x = (36725)_8$ *e* $y = (740125)_8$. *Vamos a calcular la suma de* x *e* y *y la diferencia* $y - x$.

$$\begin{array}{cccccc} & & & & {\scriptstyle 1} & \\ & 3 & 6 & 7 & 2 & 5 \\ + & 7 & 4 & 0 & 1 & 2 & 5 \\ \hline & & & & & & 2 \end{array} \qquad \begin{array}{cccccc} & & & & & \\ & 3 & 6 & 7 & 2 & 5 \\ + & 7 & 4 & 0 & 1 & 2 & 5 \\ \hline & & & & & 5 & 2 \end{array} \qquad \begin{array}{cccccc} & & & {\scriptstyle 1} & & \\ & 3 & 6 & 7 & 2 & 5 \\ + & 7 & 4 & 0 & 1 & 2 & 5 \\ \hline & & & & 7 & 0 & 5 & 2 \end{array} \qquad \begin{array}{cccccc} & & & & & \\ & 3 & 6 & 7 & 2 & 5 \\ + & 7 & 4 & 0 & 1 & 2 & 5 \\ \hline & & 7 & 7 & 7 & 0 & 5 & 2 \end{array}$$

Nótese que $x = 3 \cdot 8^4 + 6 \cdot 8^3 + 7 \cdot 8^2 + 2 \cdot 8 + 5 = 15829$, $y = 7 \cdot 8^5 + 4 \cdot 8^4 + 1 \cdot 8^2 + 2 \cdot 8 + 5 = 245845$, *luego*

$$x + y = 15829 + 245845 = 261674 = 7 \cdot 8^5 + 7 \cdot 8^4 + 7 \cdot 8^3 + 5 \cdot 8 + 2 = (777052)_8$$

$$\begin{array}{cccccc} & 7 & 4 & 0 & 1 & 2 & 5 \\ - & & 3 & {}^{1}6 & 7 & 2 & 5 \\ \hline & & & & 2 & 0 & 0 \end{array} \qquad \begin{array}{cccccc} & & 7 & 4 & 0 & 1 & 2 & 5 \\ - & & & {}^{1}3 & 6 & 7 & 2 & 5 \\ \hline & & & & 1 & 2 & 0 & 0 \end{array} \qquad \begin{array}{cccccc} & & 7 & 4 & 0 & 1 & 2 & 5 \\ - & & & 3 & 6 & 7 & 2 & 5 \\ \hline & & & 7 & 0 & 1 & 2 & 0 & 0 \end{array}$$

Para realizar una multiplicación o una división es conveniente tener las tablas de multiplicar. En base 8 éstas serían:

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	10	12	14	16
3	0	3	6	11	14	17	22	25
4	0	4	10	14	20	24	30	34
5	0	5	12	17	24	31	36	43
6	0	6	14	22	30	36	44	52
7	0	7	16	25	34	43	52	61

Ejemplo 2.1.6. *Sean* $x = (37142)_8$ *e* $y = (65)_8$. *Vamos a calcular el producto* $x \cdot y$, *y el cociente y resto que resulta de dividir* x *entre* y.

$$\begin{array}{cccccc} & & & & {\scriptstyle 1} & \\ & 3 & 7 & 1 & 4 & 2 \\ \times & & & & 6 & 5 \\ \hline & & & & & 2 \end{array} \qquad \begin{array}{cccccc} & & & & {\scriptstyle 2} & \\ & & 3 & 7 & 1 & 4 & 2 \\ \times & & & & 6 & 5 \\ \hline & & & & 5 & 2 \end{array} \qquad \begin{array}{cccccc} & & & {\scriptstyle 4} & & \\ & & 3 & 7 & 1 & 4 & 2 \\ \times & & & & 6 & 5 \\ \hline & & 3 & 7 & 5 & 2 \end{array} \qquad \begin{array}{cccccc} & & & & & \\ & & 3 & 7 & 1 & 4 & 2 \\ \times & & & & 6 & 5 \\ \hline & 2 & 3 & 3 & 7 & 5 & 2 \end{array}$$

$$\begin{array}{ccccccc} & & 3 & 7 & 1 & 4 & 2 \\ & \times & & & & 6 & 5 \\ \hline & 2 & 3 & 3 & 7 & 5 & 2 \\ 2 & 7 & 3 & 1 & 1 & 4 & \\ \hline \end{array} \qquad \begin{array}{ccccccc} & & & 3 & 7 & 1 & 4 & 2 \\ & & \times & & & & 6 & 5 \\ \hline & & 2 & 3 & 3 & 7 & 5 & 2 \\ & 2 & 7 & 3 & 1 & 1 & 4 & \\ \hline 3 & 1 & 6 & 5 & 1 & 1 & 2 & \end{array}$$

Por último, vamos a calcular la división de x *entre* y.

3 7 1 4 2 | 6 5	*Estimamos el valor de* 371 *entre* 65
	Como $5 \cdot 6 = 36$ *se queda muy próximo a* 37, *probamos por 4.*
3 7 1 4 2 | 6 5 4	$4 \cdot 5 = 24$ *hasta* 31, 5 *y nos llevamos* 3.
3 7 1 4 2 | 6 5 5 4	$4 \cdot 6 = 30$ *y* 3, 33; *hasta* 37, 4.
3 7 1 4 2 | 6 5 4 5 4	*Bajamos el* 4.
3 7 1 4 2 | 6 5 4 5 4 4	*Como antes, estimamos el valor de* 454 *entre* 65 *y ahora nos da* 5.
3 7 1 4 2 | 6 5 4 5 4 4 5	$5 \cdot 5 = 31$ *hasta* 34, 3 *y nos llevamos* 3. $5 \cdot 6 + 3 = 36 + 3 = 41$, *hasta* 45, 4. *Bajamos el* 2.
3 7 1 4 2 | 6 5 4 5 4 4 5 4 3 2	*La última cifra del cociente es* 5. *Calculamos el resto y nos da* 21.
3 7 1 4 2 | 6 5 4 5 4 4 5 5 4 3 2 2 1	

Por tanto, tenemos que $(37142)_8 = (65)_8 \cdot (455)_8 + (21)_8$.

Vamos a expresar estos números en decimal. $(37142)_8 = 15970$, $(65)_8 = 53$, $(455)_8 = 301$ *y* $(21)_8 = 17$. *Calcula el cociente y el resto de la división de* 15970 *entre* 53.

En caso de que estemos en base 2, los cálculos son mucho más sencillos, pues en tal caso, las únicas multiplicaciones que realizamos son por cero o por uno.

Ejemplo 2.1.7.

Vamos a realizar la división de dos números cuya representación en binario es $x = 101101010$ *e* $y = 1101$.

1 0 1 1 0 1 0 1 0 | 1 1 0 1	*Como* $1011 < 1101$ *tomamos una cifra más.* *Ponemos un* 1 *en el cociente y restamos:* $10110 - 1101 = 1001$.*El resultado de la resta lo situamos debajo de* 10110.
1 0 1 1 0 1 0 1 0 | 1 1 0 1 **1 0 0 1** 1	*Bajamos el* 1 *y al ser* $10011 > 1101$, *Ponemos un* 1*en el cociente y restamos:* $10011 - 1101 = 0110$. *El resultado lo situamos debajo de* 10011.

1	0	1	1	0	1	0	1	0	|	1	1	0	1
	1	0	0	1	**1**					1	**1**		
		0	**1**	**1**	**0**								

Bajamos el 0 *y como* $1100 < 1101$, 0 *al cociente y bajamos la cifra siguiente. Hacemos igual que antes.* $11001 - 1101 = 1100$.

1	0	1	1	0	1	0	1	0	|	1	1	0	1
	1	0	0	1	1					1	1	**0**	**1**
		0	1	1	0	**0**	**1**						
				1	**1**	**0**	**0**						

Por último, bajamos el 0, *llevamos un* 1 *al cociente, y colocamos el resultado de la resta* $11000 - 1101$, *que es* 1011 *bajo* 11000.

1	0	1	1	0	1	0	1	0	|	1	1	0	1	
	1	0	0	1	1					1	1	0	1	**1**
		0	1	1	0	0	1							
				1	1	0	0	**0**						
					1	**0**	**1**	**1**						

Y ya hemos terminado la división.

El cociente es $c = 11011$ *y el resto* $r = 1011$.

Si expresamos x *e* y *en el sistema decimal, nos queda que* $x = 362$ *e* $y = 13$. *Al dividir* 362 *entre* 13 *nos da de cociente* 27, *cuya expresión en binario es* 11011 *y de resto* 11, *cuya expresión en binario es* 1011.

2.2. Números enteros.

Al igual que con los números naturales comenzamos recordando algunos hechos conocidos de los números enteros.

Los números enteros forman un conjunto $\mathbb{Z}$ que contiene a $\mathbb{N}$. Dados dos números enteros, a y b, hay definidos dos nuevos números enteros, llamados respectivamente suma y producto de a y b, y representados mediante $a + b$ y $a \cdot b$ (o simplemente ab). Estas operaciones satisfacen las siguientes propiedades:

i) Para cualesquiera $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.

ii) Para cualesquiera $a, b \in \mathbb{Z}$, $a + b = b + a$.

iii) El elemento neutro para la suma en $\mathbb{N}$ es también un elemento neutro para la suma en $\mathbb{Z}$.

iv) Para cada $a \in \mathbb{Z}$ existe un elemento en $\mathbb{Z}$, representado por $-a$ tal que $a + (-a) = 0$ (Existencia de opuesto para la suma).

v) Para cualesquiera $a, b, c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

vi) Para cualesquiera $a, b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.

vii) El elemento neutro para el producto en $\mathbb{N}$ es también un elemento neutro para el producto en $\mathbb{Z}$.

viii) Si $a \cdot b = a \cdot c$ y $a \neq 0$ entonces $b = c$.

ix) Para cualesquiera $a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Nótese que la propiedad iv) implica que la suma es cancelativa. También esta propiedad permite definir la resta o diferencia de dos números enteros. Dados $a, b \in \mathbb{Z}$ se define $a - b$ como el número $a + (-b)$.

También en $\mathbb{Z}$ hay definida una relación como sigue:

$$a \leq b \text{ si } b - a \in \mathbb{N}$$

que satisface las siguientes propiedades:

x) $a \leq a$ para todo $a \in \mathbb{Z}$.

xi) Si $a \leq b$ y $b \leq a$ entonces $a = b$.

xii) Si $a \leq b$ y $b \leq c$ entonces $a \leq c$.

xiii) Para cualesquiera $a, b \in \mathbb{Z}$, $a \leq b$ o $b \leq a$.

xiv) $a \leq b$ implica que $a + c \leq b + c$ para todo $c \in \mathbb{Z}$.

xv) $a \leq b$ y $c \geq 0$ implica que $a \cdot c \leq b \cdot c$.

xvi) $a \leq b$ y $c \leq 0$ implica $b \cdot c \leq a \cdot c$.

xvii) $a \cdot c \leq b \cdot c$ y $c > 0$ entonces $a \leq b$.

xviii) $a \cdot c \leq b \cdot c$ y $c < 0$ implica que $b \leq a$.

Por último, tenemos definida la aplicación valor absoluto $|\ | : \mathbb{Z} \to \mathbb{N}$ como sigue:

$$|a| = \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a < 0 \end{cases}$$

y que satisface las propiedades:

xix) $|a| = 0$ si, y sólo si, $a = 0$.

xx) $|a \cdot b| = |a| \cdot |b|$.

xxi) $|a + b| \leq |a| + |b|$.

xxii) $|a| \leq b$ si, y sólo si, $-b \leq a \leq b$.

2.2.1. Representación en complementos

Hemos estudiado en una sección anterior cómo representar los números naturales. Esto, junto con el signo, nos permite representar todos los números enteros.

Para representar un número entero no nulo a, elegimos una base $b \geq 2$, representamos $|a|$ (que es un número natural) en base b, y le añadimos el signo $-$ al principio si el número a es menor que cero.

Sin embargo, aquí vamos a estudiar otra forma para representar los números enteros, que nos va a permitir reducir las sumas y las restas a un mismo algoritmo: el que tenemos para sumar.

Para esto, al igual que con los número naturales, elegimos un número $b \geq 2$, y vamos a trabajar en base b.

Tenemos dos posibilidades de representar los números: En complemento a $b - 1$ y en complemento a b.

Antes de explicar el caso general, vamos a analizar algunos ejemplos tomando la base que nos resulta más conocida: la base $b = 10$.

Tomemos por ejemplo $x = 75$ e $y = 28$. Su diferencia $x - y$ vale 47.

Para realizar la resta podemos proceder como sigue:

- Representamos en complemento a 9 el número y. La representación en complemento a 9 consiste en sustituir cada cifra por lo que le falta para llegar a 9. Nos quedaría entonces 71.
- Sumamos los dos números: $75 + 71 = 146$.
- Le sumamos 1 y despreciamos el acarreo (el 1 de la derecha), y nos queda 47, que es exactamente la diferencia entre x e y.

A la vista de esto, podríamos utilizar, para representar el número -28 la notación 71, a la que llamaremos *representación en complemento a 9*.

Entonces, para realizar la suma $x + (-y)$ (o lo que es lo mismo, $x - y$), lo que tenemos que hacer es sumarle a x, la representación en complemento a 9 de $-y$. El resultado final hay que interpretarlo (sumarle uno, y eliminar el acarreo)

Si analizamos lo que hemos hecho veremos porqué nos da el resultado esperado:

- Representación en complemento a 9 de $-y$. Tenemos el número $99 - y$.
- Le sumamos este número a x. $x + 99 - y = 99 + (x - y)$.
- Sumamos 1. $100 + (x - y)$
- Despreciamos el 1 de la derecha, es decir, restamos 100. $x - y$.

Supongamos ahora que queremos restar $y = 38$ a $x = 357$. Representamos $-y$ en complemento a 9 (lo que nos da 61), se lo sumamos a 357, y le sumamos 1, y nos queda $357 + 61 + 1 = 419$. La diferencia entre x e y vale 319. Para obtener este resultado a partir del cálculo que hemos hecho en complemento a 9 tendríamos que restar 1 en la cifra más significativa.

Pero esto ya parece un poco rebuscado. Además, esa regla no valdría si quisiéramos hacer $6372 - 57$ (compruébese).

Para solventar este problema, se puede tomar la opción de escribir los dos números con igual cantidad de cifras significativas. En tal caso, tendríamos $x = 357$, $y = 038$. La representación en complemento a 9 de $-y$ es 961. Ahora realizamos la suma: $357 + 961 + 1 = 1319$. El resultado de la resta $x - y$ es 319, como puede deducirse del resultado obtenido.

Tal y como hemos hecho hasta ahora, hay una ambigüedad. Supongamos que tenemos el número representado como 239. ¿Se corresponde con la representación del número *doscientos treinta y nueve*, o se corresponde con la representación del número *menos setecientos sesenta*?

Para solucionar esto, lo que hacemos es añadir una cifra a la izquierda, que será *cero* para el caso de los números positivos, y *nueve* para los negativos.

Entonces, la representación en complemento a nueve del número $x = 528$ será 0528, mientras que la de $y = -528$ será 9471.

Sabemos que si tenemos un número (positivo) y le añadimos ceros a la izquierda, el número que representamos es el mismo ($356 = 0356 = 000356$). De la misma forma, si tenemos un número negativo representado en complemento a nueve, y le añadimos *nueves* a la izquierda, el número representado es el mismo. Así, el número -356 podemos representarlo en complemento a nueve como 9643, como 99643, o como 99999643.

Y ahora, supongamos que tenemos los números $x = 37846$ e $y = 967$, y queremos calcular $x - y$.

- Representamos x en complemento a 9: 037846.
- Representamos $-y$ en complemento a 9 con el mismo número de cifras que x: 999032.
- Realizamos la suma $037846 + 999032 + 1$. El resultado es 1036879.
- Eliminamos el *uno* de la izquierda: 036879.

Luego $x - y = 36879$.

¿Que ocurre si queremos restar dos números de forma que el primero sea menor que el segundo? En tal caso, la diferencia es negativa, luego el resultado que nos dé deberemos interpretarlo como tal.

Por ejemplo, vamos a tomar $x = 45$ e $y = 123$, y vamos a calcular $x - y$.

- Representamos $-y$ en complemento a 9: 9876.
- Representamos x en complemento a 9: 0045.
- Sumamos ambos números $0045 + 9876 = 9921$.
- Puesto que el resultado empieza por *nueve* se trata de un número negativo. Su representación en complemento a 9 es 9921. Por tanto, el resultado es -78 (ya que la representación en complemento a 9 de -78 es 9921).

Al igual que antes, lo que hemos hecho ha sido sumar a x el número $9999 - y$. El resultado es $9999 + (x - y) = 9999 - (y - x)$, que es la representación en complemento a nueve de $-(y - x) = x - y$.

Vamos a ver cómo sumar y restar números que están representados en complementos. Lo primero que hemos de hacer es decidir si un número queremos sumarlo o restarlo.

Si sumamos 75 y 71, ¿queremos sumar esos dos números o lo que estamos haciendo es restar 28 a 75? Puesto que restar un número es lo mismo que sumar su opuesto, lo que necesitamos es una forma de representar los números negativos.

Para representar un número positivo en complemento a nueve, utilizamos su representación decimal y añadimos al menos un cero a la izquierda. Para los negativos, su representación en complemento a nueve consiste en sustituir en la representación de su número opuesto cada cifra por lo que le falta a ésta para llegar a 9.

Así, el 25 será representado como 025, o como 0025, etc., mientras que el -25 será representado como 974, 9974, etc.

En tal caso, si x es un número entero, y su representación en complemento a 9 es $b_n b_{n-1} \cdots b_1 b_0$, las cifras de la representación en complemento a 9 de $-x$ son $9-b_n,\ 9-b_{n-1}, \cdots 9-b_1,\ 9-b_0$.

Ejemplo 2.2.1. *Vamos a hacer algunas sumas y restas con números representados en complemento a* 9.

1. $x = 45$, $y = 26$.

   - *Para sumarlos, utilizamos la representación en complemento a* 9 *de ambos, que es* 045 *y* 026, *y la sumamos:*

   $$\begin{array}{cccc} & 0 & 4 & 5 \\ + & 0 & 2 & 6 \\ \hline & 0 & 7 & 1 \end{array}$$

   que es la representación en complemento a 9 *de la suma.*

   - *Para efectuar $x - y$ utilizamos la representación en complemento a* 9 *de x y $-y$, que son respectivamente* 045 *y* 973, *y volvemos a sumar (y sumamos también* 1*)*

   $$\begin{array}{cccc} & 0 & 4 & 5 \\ + & 9 & 7 & 3 \\ & & & 1 \\ \hline 1 & 0 & 1 & 9 \end{array}$$

   y eliminando el 1 *del acarreo, el resultado es la representación en complemento a* 9 *de la diferencia.*

   - *Para efectuar $y - x$ utilizamos la representación en complemento a* 9 *de y y $-x$, que son respectivamente* 026 *y* 954, *y sumamos:*

   $$\begin{array}{cccc} & 0 & 2 & 6 \\ + & 9 & 5 & 4 \\ \hline & 9 & 8 & 0 \end{array}$$

   que es la representación en complemento a 9 *de* -19, *es decir, $y - x$.*

   - *Para efectuar $-x - y$ utilizamos las representaciones en complemento a* 9 *de $-x$ y $-y$, que son respectivamente* 954 *y* 973. *Las sumamos y le añadimos* 1.

   $$\begin{array}{cccc} & 9 & 5 & 4 \\ + & 9 & 7 & 3 \\ & & & 1 \\ \hline 1 & 9 & 2 & 8 \end{array}$$

   y eliminando el 1 *de la derecha obtenemos la representación en complemento a* 9 *de* $-71 = -x - y$.

2. *Tomamos ahora $x = 58$ e $y = 62$. La representación en complemento a 9 de x es* 058, *la de $-x$ es* 941, *la de y es* 062 *y la de $-y$ es* 937. *Realizamos los cálculos de $x + y$, $x - y$, $-x + y = y - x$ y $-x - y$. Para ello, tomamos la representación en complemento a 9 de los cuatro números.*

   $x + y$

   $$\begin{array}{cccc} & 0 & 5 & 8 \\ + & 0 & 6 & 2 \\ \hline & 1 & 2 & 0 \end{array}$$

   $x - y$

   $$\begin{array}{cccc} & 0 & 5 & 8 \\ + & 9 & 3 & 7 \\ \hline & 9 & 9 & 5 \end{array}$$

   $-x + y$

   $$\begin{array}{cccc} & 0 & 6 & 2 \\ + & 9 & 4 & 1 \\ & & & 1 \\ \hline 1 & 0 & 0 & 4 \end{array}$$

   $-x - y$

   $$\begin{array}{cccc} & 9 & 4 & 1 \\ + & 9 & 3 & 7 \\ & & & 1 \\ \hline 1 & 8 & 7 & 9 \end{array}$$

   El primer resultado no es la representación en complemento a nueve de ningún número, pues no empieza por 0 *ni por* 9. *Si eliminamos el* uno *de la izquierda, podríamos pensar que el resultado de la suma es* 20. *En realidad, el resultado de la suma es* 120.

El segundo resultado es la representación en complemento a nueve de -4, que es el resultado de la operación $x - y$.

El tercer resultado, después de eliminar el uno *de la izquierda es* 4*, que es lo que resulta de la operación $-x + y$.*

Por último, el cuarto resultado no es la representación en complemento a nueve de ningún número, ni aún eliminando el uno *de la izquierda.*

Una opción para eliminar estos problemas es escribir los números con una cifra más, añadiendo un cero a la izquierda en el caso de los números positivos, y un 9 en el caso de los negativos.

$x + y$

$$\begin{array}{rrrrr} & 0 & 0 & 5 & 8 \\ + & 0 & 0 & 6 & 2 \\ \hline & 0 & 1 & 2 & 0 \end{array}$$

$x - y$

$$\begin{array}{rrrrr} & 0 & 0 & 5 & 8 \\ + & 9 & 9 & 3 & 7 \\ \hline & 9 & 9 & 9 & 5 \end{array}$$

$-x + y$

$$\begin{array}{rrrrr} & 0 & 0 & 6 & 2 \\ + & 9 & 9 & 4 & 1 \\ & & & & 1 \\ \hline 1 & 0 & 0 & 0 & 4 \end{array}$$

$-x - y$

$$\begin{array}{rrrrr} & 9 & 9 & 4 & 1 \\ + & 9 & 9 & 3 & 7 \\ & & & & 1 \\ \hline 1 & 9 & 8 & 7 & 9 \end{array}$$

Y ahora vemos que:

- *Como resultado de la primera operación tenemos* 0120*. Este es un número positivo, pues empieza por cero. Se trata, como sabemos del número* $120 = x + y$.
- *Como resultado de la segunda operación tenemos* 9995*. Al empezar por* nueve *se trata de un número negativo. En concreto, el número* -4*, que es el resultado de* $x - y$.
- *Al resultado de la tercera operación le quitamos el* uno *de la izquierda, y nos queda* 0004*. Al empezar por cero, se trata de un número positivo. Concretamente el* 4.
- *También al resultado de la cuarta operación le quitamos el* uno *de la izquierda. Nos queda entonces* 9879*. Al empezar por nueve se trata de un número negativo, concretamente de* -120.

Pasamos ya a dar la definición de la representación de un número en complemento a $b - 1$.

Definición 34. *Sea $b \geq 2$, x un número entero y $(a_n a_{n-1} \cdots a_1 a_0)_b$ la representación de un número en base b. Diremos que $c_n \cdots c_1 c_0$ es una representación de x en complemento a $b - 1$ si:*

- $c_n = 0$ *y* $x = (c_n c_{n-1} \cdots c_1 c_0)_b$ *cuando* $x \geq 0$.
- $c_n = b - 1$ *y* $x = (c_{n-1} \cdots c_1 c_0)_b - (b^n - 1)$ *cuando* $x < 0$.

Observaciones:

1. En la representación en complemento a $b - 1$ de un número x, la cifra de la izquierda nos indica el signo del número x.
2. Si $c_n c_{n-1} \cdots c_1 c_0$ es una representación en complemento a $b-1$ de x, entonces también $c_n c_n c_{n-1} \cdots c_1 c_0$ lo es. Es decir, podemos añadir a la izquierda tantas veces como queramos la última cifra de la representación.

   Esto es claro en el caso de que x sea un número positivo, pues lo único que hacemos es añadir un cero a la izquierda.

   Supongamos que $x < 0$, y que $c_n c_{n-1} \cdots c_1 c_0$ es una representación en complemento a $b - 1$ del número x. En tal caso, $c_n = b - 1$ y

   $$x = (c_{n-1} \cdots c_1 c_0)_b - (b^n - 1) = c_{n-1} b^{n-1} + c_{n-2} b^{n-2} + \cdots + c_1 b + c_0 - b^n + 1$$

   Sea y el número cuya representación en complemento a $b - 1$ es $c_n c_n c_{n-1} \cdots c_1 c_0$. Entonces y es negativo, pues la última cifra es $c_n = b - 1$. Por tanto,

$$\begin{aligned} y &= (c_n c_{n-1}\cdots c_1 c_0) - (b^{n+1}-1) = \\ &= c_n b^n + c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \cdots + c_1 b + c_0 - b^{n+1} + 1 = \\ &= (b-1)b^n + c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \cdots + c_1 b + c_0 - b^{n+1} + 1 = \\ &= b^{n+1} - b^n + c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \cdots + c_1 b + c_0 - b^{n+1} + 1 = \\ &= -b^n + c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \cdots + c_1 b + c_0 + 1 = x \end{aligned}$$

3. La representación de 0, de acuerdo con la definición es $00\cdots 0$. Sin embargo, también podría usarse como representación de cero $aa\cdots a$, donde $a = b-1$.

4. Con $n+1$ dígitos podemos representar todos los números comprendidos entre $-(b^n-1)$ y b^n-1.

   Sea x un número cuya representación en complemento a $b-1$ es $c_n c_{n-1}\cdots c_1 c_0$. Tenemos dos posibilidades:

   - $c_n = 0$. Entonces $x \geq 0$ y $x = (c_{n-1}\cdots c_1 c_0)_b = c_{n-1}b^{n-1} + \cdots + c_1 b + c_0 < b^n$. Es decir, $0 \leq x \leq b^n - 1$.
   - $c_n = b-1$. Entonces $x \leq 0$ y $x = c_{n-1}b^{n-1} + \cdots + c_1 b + c_0 - b^n + 1$, de donde $x + b^n - 1 = c_{n-1}b^{n-1} + \cdots + c_1 b + c_0$, luego $0 \leq x + b^n - 1 \leq b^n - 1$. Por tanto, $-(b^n-1) = -b^n + 1 \leq x \leq 0$.

   Juntando los dos casos, tenemos que $-(b^n-1) \leq x \leq b^n - 1$.

5. Si $c_n c_{n-1}\cdots c_1 c_0$ es la representación en complemento a $b-1$ de x, entonces la representación en complemento a $b-1$ de $-x$ es $d_n d_{n-1}\cdots d_1 d_0$, donde $d_i = (b-1) - c_i$. Esto vale, tanto si x es positivo como si x es negativo.

   Sea x un número cuya representación en complemento a $b-1$ es $c_n c_{n-1}\cdots c_1 c_0$. Sea y el número cuya representación en complemento a $b-1$ es $d_n d_{n-1}\cdots d_1 d_0$, donde $d_i = (b-1) - c_i$. Entonces:

   - Si $x \geq 0$ se tiene que $c_n = 0$, luego $d_n = b-1$, lo que nos dice que y es negativo. Ahora:

     $$\begin{aligned} y &= d_{n-1}b^{n-1} + d_{n-2}b^{n-2} + \cdots + d_1 b + d_0 - b^n + 1 = \\ &= ((b-1) - c_{n-1})b^{n-1} + ((b-1) - c_{n-2})b^{n-2} + \cdots ((b-1) - c_1)b + (b-1) - c_0 - b^n + 1 = \\ &= (b-1)(b^{n-1} + b^{n-2} + \cdots + b + 1) - (c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \cdots + c_1 b + c_0) - b^n + 1 = \\ &= b^n + b^{n-1} + \cdots + b - (b^{n-1} + b^{n-2} + \cdots + b + 1) - x - b^n + 1 = \\ &= b^n - 1 - x - b^n + 1 = -x \end{aligned}$$

   - Si $x \leq 0$ se procede de forma análoga. Ahora $c_n = b-1$, luego $d_n = 0$, lo que nos dice que $y \geq 0$.

     $$\begin{aligned} x &= c_{n-1}b^{n-1} + c_{n-2}b^{n-2} + \cdots + c_1 b + c_0 - b^n + 1 = \\ &= ((b-1) - d_{n-1})b^{n-1} + ((b-1) - d_{n-2})b^{n-2} + \cdots ((b-1) - d_1)b + (b-1) - d_0 - b^n + 1 = \\ &= (b-1)(b^{n-1} + b^{n-2} + \cdots + b + 1) - (d_{n-1}b^{n-1} + d_{n-2}b^{n-2} + \cdots + d_1 b + d_0) - b^n + 1 = \\ &= b^n + b^{n-1} + \cdots + b - (b^{n-1} + b^{n-2} + \cdots + b + 1) - y - b^n + 1 = \\ &= b^n - 1 - y - b^n + 1 = -y \end{aligned}$$

   Luego en cualquiera de los casos, $y = -x$.

Ejemplo 2.2.2.

1. *Vamos a ver algunos ejemplos de representaciones en complemento a* nueve.

   Sea x el número cuya representación en complemento a nueve es 0583. *Entonces x es positivo, pues la cifra de la izquierda es* 0. *Y se tiene que* $x = 5\cdot 10^2 + 8\cdot 10 + 3 = 583$.

   Ahora sustituimos cada cifra por lo que le falta para llegar a 9 *(es decir, sustituimos cada cifra c_i por $9 - c_i$. En este caso, tenemos el número* 9416. *Esta es la representación en complemento a nueve de un número negativo, pues empieza por* 9. *Este número, de acuerdo con la definición 34 es* $4\cdot 10^2 + 1\cdot 10 + 6 - 10^3 + 1 = -583$.

Sea z el número cuya representación en complemento a nueve es 999416. *Entonces, según la definición 34 se tiene que*

$$z = 9 \cdot 10^4 + 9 \cdot 10^3 + 4 \cdot 10^2 + 1 \cdot 10 + 6 - 10^5 + 1 = 99416 - 99999 = -583.$$

También podríamos haber procedido de la siguiente forma: el número z es negativo, pues empieza por 9. *Representamos $-z$, que se consigue cambiando cada cifra por lo que le falta para llegar a* 9. *Entonces, la representación de $-z$ es* 000583. *Luego $-z = 583$, de donde $z = -583$.*

4734 *no es la representación en complemento a nueve de ningún número, pues su primera cifra no es ni cero ni nueve.*

2. *Un caso especialmente interesante y sencillo es cuando trabajamos en complemento a* uno. *En tal caso, una sucesión de* ceros *y* unos *es siempre la representación en complemento a* uno *de algún número, que será positivo si la primera cifra es cero, y negativo si la primera cifra es uno. Una sucesión de n dígitos se corresponde con un número entre $-(2^{n-1} - 1)$ y $2^{n-1} - 1$.*

   Vamos a representar en complemento a uno, todos los números entre $-7 = -(2^3 - 1)$ y $7 = 2^3 - 1$ con cuatro dígitos. Pondremos juntas la representación de un número y su opuesto.

$$\begin{array}{cccc} 1 \mapsto 0001 & 2 \mapsto 0010 & 3 \mapsto 0011 & 4 \mapsto 0100 \\ -1 \mapsto 1110 & -2 \mapsto 1101 & -3 \mapsto 1100 & -4 \mapsto 1011 \end{array}$$

$$\begin{array}{ccc} 5 \mapsto 0101 & 6 \mapsto 0110 & 7 \mapsto 0111 \\ -5 \mapsto 1010 & -6 \mapsto 1001 & -7 \mapsto 1000 \end{array} \qquad 0 \mapsto 0000$$

   Nos queda la secuencia 1111, *que como ya hemos dicho antes, se correspondería con el número* 0 *(o con el -0).*

   Vemos como para obtener la representación en complemento a uno *de $-x$ a partir de la de x basta intercambiar los ceros por unos y viceversa.*

Para sumar dos números x e y, positivos o negativos, podemos tomar la representación en complemento a $b-1$ de ambos números y sumarlos, teniendo en cuenta:

1. Ambos números deben tener el mismo número de cifras. Caso de no ser así, podemos repetir la cifra de la izquierda tantas veces como nos convenga.

2. Las dos últimas cifras deben ser iguales. Esto no siempre es necesario, pero de esta forma nos evitamos algunos errores.

3. Si sumamos dos números negativos, o si sumamos un positivo con un negativo de menor valor absoluto, al resultado final hay que sumarle uno, y eliminar el uno que nos aparece a la izquierda (del acarreo).

Con estas consideraciones, el resultado de la suma es la representación en complemento a $b-1$ de $x+y$.

Ejemplo 2.2.3.
Vamos a realizar algunas sumas trabajando con la representación en complemento a 1 *de los números.*

1. *Vamos a sumar $x = 45$ e $y = 89$. Para buscar su representación en complemento a* 1, *los pasamos a binario, y luego completamos las cifras. Omitiremos los subíndices, para no complicar la notación.*

Decimal	*Binario*	*Complemento a* 1	*Completando cifras*
45	101101	0101101	000101101
89	1011001	01011001	001011001

   Y ahora sumamos:

$$\begin{array}{cccccccccc} & & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & & {\scriptstyle 1} & \\ & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ + & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ \hline & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}$$

Y la representación en complemento a uno *de* $x+y$ *es* 010000110*, que se corresponde con el número* 134*.*

2. $x = 54$, $y = -87$.

   Procedemos igual que antes, pero para obtener la representación en complemento a uno de y*, pasamos por la representación binaria de* $|y|$*.*

Decimal (N)	*Binario* $(\|N\|)$	*Complemento a* 1 $(\|N\|)$	*Complemento a* 1 (N)	*Completando cifras*
54	110110	0110110	0110110	000110110
-87	1010111	01010111	10101000	110101000

$$\begin{array}{cccccccccc} & & & {\scriptstyle 1} & & & & & & \\ & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ + & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ \hline & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}$$

Y esta es la representación en complemento a uno de $x+y$*. Para obtener su representación decimal, podemos:*

- *Calculamos su opuesto, cuya representación en complemento a uno es* 000100001 *que es el número* $2^5 + 1 = 33$*. Por tanto,* $x + y = -33$*.*
- *Obtenerlo directamente de la representación.* $x+y = 2^7+2^6+2^4+2^3+2^2+2^1-2^8+1 = -33$*.*

3. $x = 61$, $y = -34$.

Decimal (N)	*Binario* $(\|N\|)$	*Complemento a* 1 $(\|N\|)$	*Complemento a* 1 (N)	*Completando cifras*
61	111101	0111101	0111101	00111101
-34	100010	0100010	1011101	11011101

$$\begin{array}{cccccccccc} & & & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & {\scriptstyle 1} & \\ & & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ + & & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ \hline & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{array}$$

Y como nos ha salido una cifra más, la quitamos y sumamos uno. El resultado es entonces 00011011*, que es la representación en complemento a uno de* 27*.*

4. $x = -39$, $y = -52$.

Decimal (N)	*Binario* $(\|N\|)$	*Complemento a* 1 $(\|N\|)$	*Complemento a* 1 (N)	*Completando cifras*
-39	100111	0100111	1011000	11011000
-52	110100	0110100	1001011	11001011

$$\begin{array}{cccccccccc} & & & {\scriptstyle 1} & & {\scriptstyle 1} & {\scriptstyle 1} & & & \\ & & & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ + & & & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ \hline & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{array}$$

Y al igual que antes, como nos ha salido una cifra más, la quitamos y sumamos uno. El resultado de la suma $x+y$ *es entonces* 10100100*, que es la representación en complemento a uno del número* $2^5 + 2^2 - 2^7 + 1 = -91$*.*

Para evitar los problemas que pueden surgir de la necesidad de sumar o no 1 según los casos, se suele emplear más que la representación en complemento a $b-1$ la representación en complemento a b. En este caso, lo que se hace es "incluir" el uno en la representación del número.

Para obtener la representación en complemento a b de un número x:

- si el número es positivo, la representación en complemento a b de un número es la misma que la representación en complemento a $b-1$.
- si x es negativo, se toma la representación en complemento a $b-1$ de x y se le suma 1.

Dicho de otra forma, si $c_nc_{n-1}\cdots c_1c_0$ es la representación en complemento a b de x, entonces $c_n = 0$ ó $c_n = b-1$, y:

- si $c_n = 0$, $x = (c_nc_{n-1}\cdots c_1c_0)_b$.
- si $c_n = b-1$, $x = (c_{n-1}\cdots c_1c_0)_b - b^n$.

Definición 35. *Sea $b \geq 2$, x un número entero y $(a_na_{n-1}\cdots a_1a_0)_b$ la representación de un número en base b. Diremos que $c_n\cdots c_1c_0$ es una representación de x en complemento a b si:*

- $c_n = 0$ *y* $x = (c_nc_{n-1}\cdots c_1c_0)_b$ *cuando* $x \geq 0$.
- $c_n = b-1$ *y* $x = (c_{n-1}\cdots c_1c_0)_b - b^n$ *cuando* $x < 0$.

Observaciones:

1. El decir representación en complemento a *un número* podría ser ambiguo. Por ejemplo, si hablamos de representación en complemento a 2, podríamos estar utilizando la base $b = 3$ y usar la representación en complemento a $b-1$, o utilizar la base $b = 2$ y usar la representación en complemento a b. Puesto que nosotros usaremos la base $b = 2$ ó $b = 10$, no tendremos este problema.
2. En la representación en complemento a b de un número x, la cifra de la izquierda nos indica el signo del número x.
3. Si $c_nc_{n-1}\cdots c_1c_0$ es una representación en complemento a b de x, entonces también $c_nc_nc_{n-1}\cdots c_1c_0$ lo es. Es decir, podemos añadir a la izquierda tantas veces como queramos la última cifra de la representación.
4. Con $n+1$ dígitos podemos representar todos los números comprendidos entre $-b^n$ y $b^n - 1$.
5. Si $c_nc_{n-1}\cdots c_1c_0$ es la representación en complemento a b de x, para obtener la representación en complemento a b de $-x$ sustituimos cada cifra c_i por $d_i = (b-1)-c_i$ y sumamos 1 al resultado, como si estuviéramos trabajando con un número en base b. Esto vale para todos los números comprendidos entre $-b^n$ y $b^n - 1$ salvo para $x = 0$ (la representación de 0 y -0 es, obviamente la misma) y para $x = -b^n$ (pues $-x = b^n$, que no puede representarse con $n+1$ cifras).

Ejemplo 2.2.4.

1. *Vamos a obtener la representación en complemento a 10 de varios números enteros.*
   - $x = 37$. *Una representación en complemento a 10 es* 037. *También podemos tomar* 0037, 00037, *etc.*
   - *Sea* $x = -83$. *El número* $-x$, *representado en complemento a* 10 *es* 083, *luego la representación de* x *es* $916 + 1 = 917$.
   - *Sea* $x = 1000$ *(es decir,* b^3*). Entonces su representación en complemento a* 10 *es* 01000. *Necesitamos 5 cifras para representar* b^3.
   - *Sea ahora* $x = -1000$. *Los pasos para representarlo serían:*

     Representamos $-x = 1000$. *Esto nos da* 01000.
     Sustituimos cada cifra por su complemento a 9. Nos da 98999.
     Sumamos 1. Y nos da 99000

Entonces, una representación de -1000 *sería* 99000. *Pero también lo es* 9000 *(pues 9000 y 99000 representan el mismo número, ya que se ha añadido un 9 a la izquierda en la representación de un número negativo). Por tanto, vemos como* -10^3 *podemos representarlo con 4 cifras.*

2. *Sea ahora* x *un número entero cuya representación en complemento a 10 es* 9673. *Entonces, para representar* $-x$ *sustituimos cada cifra por su complemento a 9 (0326) y sumamos uno (0327). De aquí sacamos que* $x = -327$.

   También podemos verlo, según la definición 35, calculando $x = 673 - 10^3 = 673 - 1000 = -327$.

3. *La representación de* -3200 *sería* 96800 *(de* $96799 + 1$*).*

4. *En el caso de complemento a 2, se procede de forma análoga.*

El objetivo de la introducción de las representaciones en complementos viene dada por el siguiente teorema.

Teorema 2.2.1. *Sea* $b \geq 2$ *y sean* x *e* y *dos números enteros, tales que sus representaciones en complemento a* b *son* $c_n c_{n-1} \cdots c_1 c_0$ *y* $d_n d_{n-1} \cdots d_1 d_0$ *y además* $c_n = c_{n-1}$ *y* $d_n = d_{n-1}$.

Sea $s_{n+1} s_n s_{n-1} \cdots s_1 s_0$ *el resultado de realizar la suma en base* b *de los números* $c_n c_{n-1} \cdots c_1 c_0$ *y* $d_n d_{n-1} \cdots d_1 d_0$.

Entonces, $s_n s_{n-1} \cdots s_1 s_0$ *es una representación en complemento a* b *del número* $x + y$.

Ejemplo 2.2.5.

Vamos a realizar sumas de números representados en complemento a dos.

En primer lugar, $x = 38$ *e* $y = -21$. *La representación en complemento a 2 de 38 es* 0100110 *y la de* 21 *es* 010101, *por lo que la de* -21 *es* $101010 + 1 = 101011$. *Sumamos ambos números*

$$\begin{array}{cccccccccc} & & {\scriptstyle 1} & {\scriptstyle 1} & & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & \\ & & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ + & & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ \hline & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}$$

Como nos ha salido una cifra más, la eliminamos, y el resultado es 00010001, *que es una representación del número* 17.

Sean ahora $x = -25$ *e* $y = -43$. *La representación en complemento a dos de 25 es* 011001, *y la de* 43 *es* 0101011, *luego la representación de* x *es* $100110 + 1 = 100111$ *y la de* y *es* $1010100 + 1 = 1010101$. *Sumamos:*

$$\begin{array}{cccccccccc} & & {\scriptstyle 1} & & & & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & \\ & & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ + & & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}$$

Y al igual que antes, suprimimos la cifra que nos ha salido, y tenemos el resultado, que es 10111100, *que es la representación en complemento a 2 de* -68 *(bastaría cambiar los* unos *por* ceros, *los* ceros *por* unos, *y sumar uno.*

Si aquí no hubiéramos añadido una cifra a la izquierda, habríamos sumado los números 1100111 *y* 1010101, *cuyo resultado es* 10111100. *Después de eliminar el* uno *del acarreo, habríamos obtenido* 0111100, *que es la representación en complemento a dos de* 60.

Para sumar los números cuya representación en complemento a dos es 011011 y 1011, lo que hemos de hacer es completar con cifras a la izquierda hasta que los dos tengan el mismo número de cifras, y las dos últimas sean iguales. Entonces tendríamos los números 0011011 *y* 1111011, *que al sumarlos nos da* 10010110. *Como nos ha salido una cifra de más (hemos pasado de 7 a 8 cifras), eliminamos la de la izquierda, y lo que nos quede es el resultado de la suma en complemento a 2. En este caso es* $0010110 = 010110$ *que es el número 22.*

Representa los dos números iniciales en decimal y efectúa la operación.

2.3. Divisibilidad

Veíamos en la sección anterior que dados dos números naturales a, b con $b \neq 0$ podíamos dividir a entre b obteniendo un cociente y un resto (teorema 2.1.2). Ahora vamos a extender ese teorema al caso de los números enteros.

Teorema 2.3.1. *Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen únicos números enteros c, r tales que $a = bc + r$ y $0 \leq r < |b|$.*

A los números c y r que nos da el teorema se les llama respectivamente cociente y resto de la división de a entre b.

Para demostrar el teorema, lo que hay que hacer es distinguir casos según sean a y b mayores o menores que 0 y referirse al caso conocido ($a, b \in \mathbb{N}$). El siguiente ejemplo puede ayudar a analizar los diferentes casos.

Ejemplo 2.3.1.

$a = 86,\ b = 15.$ $\quad 86 = 15 \cdot 5 + 11$

$a = 86,\ b = -15.$ $\quad 86 = (-15) \cdot (-5) + 11$

$a = -86,\ b = 15.$ $\quad -86 = 15 \cdot (-6) + 4$

$a = -86,\ b = -15.$ $\quad -86 = (-15) \cdot (-6) + 4$

Ahora podemos tomar la definición 32 y extenderla a los números enteros.

Definición 36. *Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Definimos los números a div b y a mód b como el cociente y el resto de la división de a entre b respectivamente.*

Dicho de otra forma, a div b y a mód b son los únicos números que cumplen las dos condiciones siguientes:

- $a = b \cdot (a \text{ div } b) + (a \text{ mód } b)$.
- $0 \leq a \text{ mód } b < |b|$.

> Tal y como lo hemos definido aquí, el resto de una división es siempre un número positivo (o cero) y menor que el divisor (en valor absoluto). En algunas ocasiones, es conveniente tomar el resto de la división entra a y b como el número de menor valor absoluto r tal que $a - r$ es múltiplo de b. Esto daría lugar a restos negativos. Por ejemplo, al dividir 14 entre 5, nosotros tomamos como resto 4, que viene de la igualdad $14 = 5 \cdot 2 + 4$. Pero también podríamos apoyarnos en $14 = 5 \cdot 3 + (-1)$, en cuyo caso el resto sería -1. En este caso, los posibles restos al dividir por 5 serían -2, -1, 0, 1 y 2.

Pasamos ya a definir la relación de divisibilidad en $\mathbb{Z}$.

Definición 37. *Dados $a, b \in \mathbb{Z}$, se dice que a divide a b, o que b es un múltiplo de a, y escribiremos $a|b$, si existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$.*

Hagamos un repaso de las propiedades más importantes, y cuya demostración es casi inmediata.

Propiedades:

1. Para cualquier $a \in \mathbb{Z}$ se verifica que $1|a$ y $a|0$.
2. Para cualquier $a \in \mathbb{Z}$, $a|a$.
3. Si $a|b$ y $b|a$ entonces $a = \pm b$.
4. Si $a|b$ y $b|c$ entonces $a|c$.
5. Si $a|b$ y $a|c$ entonces $a|(b + c)$.
6. Si $a|b$ entonces $a|bc$ para cualquier $c \in \mathbb{Z}$.
7. $a|b$ si, y sólo si, b mód $a = 0$ (esto vale siempre que $a \neq 0$, pues en caso contrario no tiene sentido hablar de b mód a).

Según la definición que acabamos de dar, si $a|b$ existe un elemento c tal que $b = a \cdot c$. Este elemento, salvo cuando $a = 0$ está totalmente determinado por a y b. Lo denotaremos entonces como $\frac{b}{a}$.

Aunque estamos usando una notación de fracción, en este contexto $\frac{b}{a}$ sólo tiene sentido cuando $a|b$, en cuyo caso es un elemento de $\mathbb{Z}$.

Definición 38. *Sean a, b dos números enteros. Se dice que d es un máximo común divisor de a y b si se satisfacen las dos siguientes condiciones:*

- *$d|a$ y $d|b$.*
- *Si $c|a$ y $c|b$ entonces $c|d$.*

Nótese que la primera condición nos dice que d debe ser un divisor común de a y b. La segunda condición nos dice que de todos los divisores comunes es el "más grande".

Nótese también que si d es un máximo común divisor de a y b, también lo es $-d$, de ahí que hayamos hablado de **un** máximo común divisor y no de **el** máximo común divisor. Además, si d es un máximo común divisor, no hay otro máximo común divisor aparte de $-d$. Dados $a, b \in \mathbb{Z}$, denotaremos por $mcd(a, b)$ al único máximo común divisor de a y b que pertenece a $\mathbb{N}$.

Ejemplo 2.3.2. *Sean $a = 16$ y $b = 30$. Los divisores de a son $\{\pm1, \pm2, \pm4, \pm8, \pm16\}$, y los divisores de 30 son $\{\pm1, \pm2, \pm3, \pm5, \pm6, \pm10, \pm15, \pm30\}$.*

La intersección de ambos conjuntos, es decir, el conjunto de los divisores comunes, es el conjunto $\{1, 2, -1, -2\}$

De esos cuatro, tanto el 2 como el -2 son múltiplos del resto, luego podemos decir de cualquiera de los dos que es un máximo común divisor de 16 y 30.

No obstante, diremos que el máximo común divisor de 16 y 30 es 2 (es decir, elegiremos el positivo, aunque podríamos haber hecho lo mismo con el negativo).

De la misma forma que se ha definido el máximo común divisor de dos números podría hacerse para tres o más.

La definición del mínimo común múltiplo es semejante a la que acabamos de dar.

Definición 39. *Sean a, b dos números enteros. Se dice que m es un mínimo común múltiplo de a y b si se satisfacen las dos siguientes condiciones:*

- *$a|m$ y $b|m$.*
- *Si $a|n$ y $b|n$ entonces $m|n$.*

Las mismas observaciones que se han hecho para el máximo común divisor valen ahora para el mínimo común múltiplo.

Algunas propiedades referentes al máximo común divisor son:

Propiedades:

1. $mcd(a, b) = mcd(a, -b) = mcd(-a, b) = mcd(-a, -b) = mcd(|a|, |b|)$.
2. $mcd(a, 0) = |a|$ y $mcd(a, 1) = 1$
3. Si $a|b$ entonces $mcd(a, b) = |a|$.
4. $mcd(a, mcd(b, c)) = mcd(mcd(a, b), c) = mcd(a, b, c)$.
5. $mcd(ac, bc) = mcd(a, b) \cdot |c|$
6. Si $d|a$ y $d|b$ entonces $mcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{mcd(a,b)}{|d|}$.

Se deja como ejercicio enunciar las propiedades correspondientes al mínimo común múltiplo.

Hasta ahora hemos hablado del máximo común divisor, y hemos dado algunas propiedades. Estas propiedades podrían, en un principio, no tener sentido, pues el máximo común divisor de dos números podría no existir. Veremos a continuación que el máximo común divisor de dos números enteros existe, y daremos un método para calcularlo. Comenzamos con el siguiente lema.

Lema 2.3.1. *Sean $a, b \in \mathbb{Z}$. Entonces, para cualquier $q \in \mathbb{Z}$ se tiene que $mcd(a, b) = mcd(b, a - bq)$.*

Demostración: Sea $d \in \mathbb{Z}$, y supongamos que $d|a$ y $d|b$. Entonces $d|bq$, luego $d|b$ y $d|(a - bq)$.

Por otra parte si suponemos que $d|b$ y $d|(a - bq)$ deducimos que $d|bq$, luego $d|(a - bq + bq)$ y $d|b$, es decir, $d|a$ y $d|b$. ■

Nótese que lo que hemos demostrado es que para cualquier $q \in \mathbb{Z}$, los divisores comunes de a y b, y los divisores comunes de b y $a - bq$ son los mismos, luego el máximo común divisor de ambas parejas de números será el mismo (si existe).

Ejemplo 2.3.3. *Sean $a = 78$ y $b = 30$. El conjunto de los divisores positivos de a es el conjunto $\{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$, mientras que $\{1, 2, 3, 5, 6, 10, 15, 30\}$ es el conjunto de los divisores positivos de b.*

Por tanto, el conjunto de los divisores comunes de a y b es $\{1, -1, 2, -2, 3, -3, 6, -6\}$ y de ahí deducimos que $mcd(a, b) = 6$.

Vamos a tomar diferentes valores de q, y a calcular los divisores de b y $a - bq$.

- *$q = 1$. En tal caso, $a - bq = 48$. Los divisores positivos de 48 son $1, 2, 3, 4, 6, 8, 12, 16, 24, 48$. Los divisores comunes de b y $a - bq$ son los elementos del conjunto $\{1, -1, 2, -2, 3, -3, 6, -6\}$, exactamente igual que para a y b. Por tanto, $mcd(a, b) = mcd(b, a - b)$.*
- *$q = 2$. Ahora $a - bq = 18$, que tiene como divisores positivos a $1, 2, 3, 6, 9, 18$. El conjunto de los divisores comunes entre b y $a - bq$ vuelve a ser $\{1, -1, 2, -2, 3, -3, 6, -6\}$.*
- *$q = 3$. Ahora $a - bq = -12$, y el conjunto de los divisores positivos de -12 es $\{1, 2, 3, 4, 6, 12\}$. Al igual que antes, los divisores comunes de b y $a - bq$ son $1, -1, 2, -2, 3, -3, 6, -6$.*
- *$q = -2$. Entonces $a - bq = 138$. El conjunto de sus divisores positivos es $\{1, 2, 3, 6, 23, 46, 69, 138\}$ y los comunes vuelven a ser los mismos.*
- *El caso $q = 0$ es un caso trivial.*

Vemos como, independientemente del número q que tomemos, los divisores comunes de a y b son los mismos que los divisores comunes de b y $a - bq$.

El papel de a y b es simétrico, luego los divisores comunes de a y b son los divisores comunes de a y $b - aq$.

Consecuencia inmediata del lema anterior es el siguiente corolario.

Corolario 2.3.1. *Sean $a, b \in \mathbb{Z}$, con $a \neq 0$. Entonces $mcd(a, b) = mcd(b, a \text{ mód } b)$.*

Basta tomar como valor de q el cociente de a entre b.

Este resultado es en el que nos vamos a apoyar para dar el siguiente algoritmo.

Algoritmo de Euclides para el cálculo del máximo común divisor.

Sean $a, b \in \mathbb{Z}$. Puesto que $mcd(a, b) = mcd(|a|, |b|)$, podemos suponer que $a, b \in \mathbb{N}$. Comenzamos a efectuar divisiones:

$$\begin{aligned}
a &= b \cdot c_1 + r_1 \\
b &= r_1 \cdot c_2 + r_2 \\
r_1 &= r_2 \cdot c_3 + r_3 \\
&\cdots\cdots\cdots\cdots\cdots \\
r_{i-2} &= r_{i-1} \cdot c_i + r_i \\
&\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

Obtenemos una sucesión de números naturales $r_1, r_2 \cdots$, que es decreciente. Deberá por tanto existir $k \in \mathbb{N}$ tal que $r_k \neq 0$ y $r_{k+1} = 0$. Tenemos entonces:

$$\begin{aligned}
a &= b \cdot c_1 + r_1 \\
b &= r_1 \cdot c_2 + r_2 \\
r_1 &= r_2 \cdot c_3 + r_3 \\
&\cdots\cdots\cdots\cdots\cdots \\
r_{i-2} &= r_{i-1} \cdot c_i + r_i \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
r_{k-2} &= r_{k-1} \cdot c_k + r_k \\
r_{k-1} &= r_k \cdot c_{k+1} + 0
\end{aligned}$$

Por el corolario anterior tenemos que los divisores comunes de a y b coinciden con los divisores comunes de r_i y r_{i+1}, para cualquier $i \leq k$. Como el máximo común divisor de r_k y 0 existe, y vale r_k, deducimos que $mcd(a,b) = r_k$ (el último resto no nulo).

Con esto es posible diseñar un algoritmo que calcule el máximo común divisor de dos números enteros a y b.

Algoritmo EUCLIDES(a,b)

Entrada: $a, b \in \mathbb{Z}$

Salida: $d = mcd(a,b)$

$(a,b) := (|a|, |b|)$
Mientras $b \neq 0$
$(a,b) := (b, a \text{ mód } b)$
Devuelve a

Ejemplo 2.3.4. *Vamos a calcular el máximo común divisor de* 48 *y* 30. *Al ser a y b positivos, no es necesario ejecutar la primera sentencia.*

$(a,b) = (48,30)$ *Al ser* $b = 30 \neq 0$ *hacemos*
$(a,b) = (30,18)$ *Como* $b = 18 \neq 0$ *hacemos*
$(a,b) = (18,12)$ *Dado que* $b = 12 \neq 0$ *hacemos*
$(a,b) = (12,6)$ *Puesto que* $b = 6 \neq 0$ *hacemos*
$(a,b) = (6,0)$ *Y ahora* $b = 0$

Por tanto, el máximo común divisor de 48 *y* 30 *es* $a = 6$.

Teorema 2.3.2. *[Identidad de Bezout] Sean $a, b \in \mathbb{Z}$ y $d = mcd(a,b)$. Entonces existen $u, v \in \mathbb{Z}$ tales que $d = au + bv$.*

Demostración: Sabemos que el cálculo del máximo común divisor de a y b lo podemos realizar mediante una serie de divisiones

$$\begin{aligned}
r_{-1} &= r_0 \cdot c_1 + r_1 \\
r_0 &= r_1 \cdot c_2 + r_2 \\
r_1 &= r_2 \cdot c_3 + r_3 \\
&\cdots\cdots\cdots\cdots\cdots \\
r_{i-2} &= r_{i-1} \cdot c_i + r_i \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
r_{k-2} &= r_{k-1} \cdot c_k + r_k \\
r_{k-1} &= r_k \cdot c_{k+1} + 0
\end{aligned}$$

donde $r_{-1} = a$ y $r_0 = b$. Vamos a demostrar que para cada i tal que $-1 \leq i \leq k$ existen $u_i, v_i \in \mathbb{Z}$ tales que $r_i = a \cdot u_i + b \cdot v_i$.

Claramente, para $i = -1$ e $i = 0$ el resultado es cierto, pues
$r_{-1} = a \cdot 1 + b \cdot 0$ y $r_0 = a \cdot 0 + b \cdot 1$ (es decir, $(u_{-1}, v_{-1}) = (1,0)$ y $(u_0, v_0) = (0,1)$).

Supongamos que para todo $j < i$ existen u_j y v_j tales que $r_j = a \cdot u_j + b \cdot v_j$. Entonces:

$$\begin{aligned}
r_i &= r_{i-2} - r_{i-1} \cdot c_i \\
&= (a \cdot u_{i-2} + b \cdot v_{i-2}) - (a \cdot u_{i-1} + b \cdot v_{i-1}) \cdot c_i \\
&= a \cdot (u_{i-2} - u_{i-1} \cdot c_i) + b \cdot (v_{i-2} - v_{i-1} \cdot c_i)
\end{aligned}$$

Basta entonces tomar $u_i = u_{i-2} - u_{i-1} \cdot c_i$ y $v_i = v_{i-2} - v_{i-1} \cdot c_i$ ■

Esta demostración además nos dice cómo encontrar los coeficientes u y v.

Ejemplo 2.3.5. *Vamos a hallar el máximo común divisor de* 1005 *y* 450, *y a expresarlo en función de estos dos números.*

Realizamos las divisiones, y a la vez vamos expresando los restos en funciónde 1005 *y* 450.

$1005 = 450 \cdot 2 + 105$ $\qquad$ $105 = 1005 \cdot 1 + 450 \cdot (-2)$

$450 = 105 \cdot 4 + 30$

$$\begin{aligned} 30 &= 450 - 105 \cdot 4 = 450 - (1005 \cdot 1 + 450 \cdot (-2)) \cdot 4 \\ &= 1005 \cdot (-4) + 450 \cdot (1 - (-2) \cdot 4) \\ &= 1005 \cdot (-4) + 450 \cdot 9 \end{aligned}$$

$105 = 30 \cdot 3 + 15$

$$\begin{aligned} 15 &= 105 - 30 \cdot 3 = (1005 \cdot 1 + 450 \cdot (-2)) - (1005 \cdot (-4) + 450 \cdot 9) \cdot 3 \\ &= 1005 \cdot (1 - (-4) \cdot 3) + 450 \cdot (-2 - 9 \cdot 3) \\ &= 1005 \cdot (13) + 450 \cdot (-29) \end{aligned}$$

$30 = 15 \cdot 2 + 0$

De donde deducimos que $mcd(1005, 450) = 15$, *y* $15 = 1005 \cdot 13 + 450 \cdot (-29)$.

Estos datos pueden ser ordenados como sigue:

r	c	u	v
1005		*1*	*0*
450		*0*	*1*
105	*2*	*1*	*-2*
30	*4*	*-4*	*9*
15	*3*	*13*	*-29*
0			

$1005 = 1 \cdot 1005 + 0 \cdot 450$
$450 = 0 \cdot 1005 + 1 \cdot 450$
$105 = 1 \cdot 1005 - 2 \cdot 450$
$30 = -4 \cdot 1005 + 9 \cdot 450$
$15 = 13 \cdot 1005 - 29 \cdot 450$

A la derecha de la tabla hemos puesto las comprobaciones de que el primer elemento de cada fila es igual a a por el tercero más b por el cuarto, es decir, $r_i = a \cdot u_i + b \cdot v_i$.

El siguiente algoritmo recoge todos estos cálculos. Este algoritmo calcula, dados $a, b \in \mathbb{Z}$ su máximo común divisor d y los coeficientes u y v tales que $d = au + bv$.

Puesto que en el cálculo de u_i es necesario tener presente los valores de u_{i-1} y u_{i-2} necesitaremos de una variable x donde almacenar u_{i-2}. De la misma forma necesitaremos una variable y para almacenar v_{i-2}.

Algoritmo BEZOUT(a, b)
Entrada: $a, b \in \mathbb{Z}$
Salida: (d, u, v): $d = mcd(a, b)$; $d = au + bv$
  Si $b = 0$
    Devuelve $(a, 1, 0)$;
    Fin
  $r_{-1} := a$, $r_0 := b$.
  $u_{-1} := 1$, $u_0 := 0$.
  $v_{-1} := 0$, $v_0 := 1$.
  $i := 1$.
  $r_1 := r_{-1}$ mód r_0
  Mientras $r_i \neq 0$
    $c_i := r_{i-2}$ div r_{i-1}.
    $u_i := u_{i-2} - u_{i-1} \cdot c_i$.
    $v_i := v_{i-2} - v_{i-1} \cdot c_i$.
    $i := i + 1$.
    $r_i := r_{i-2}$ mód r_{i-1}.
  Devuelve $(r_{i-1}, u_{i-1}, v_{i-1})$.
  Fin

En el caso de que a ó b valieran cero, en el resultado final podría devolver un valor para d negativo. Bastaría entonces multiplicar d, u y v por -1.

Ejemplo 2.3.6.

Vamos a tomar $a = 69$ *y* $b = 15$*, y vamos a calcular su máximo común divisor,* d*, así como los coeficientes* u *y* v *que verifican que* $d = 69 \cdot u + 15 \cdot v$*.*

Puesto que $b \neq 0$*, inicializamos las variables:* $r_{-1} = 69$*,* $r_0 = 15$*,* $u_{-1} = 1$*,* $u_0 = 0$*,* $v_{-1} = 0$ *y* $v_0 = 1$*. Una vez hecho esto,* $r_1 = 69$ *mód* $15 = 9$*.*

i	r	c	u	v
-1	69		1	0
0	15		0	1
1	9			

Puesto que $r_i = r_1 = 9 \neq 0$*, volvemos a entrar en el bucle. Esto nos da* $c_1 = 69$ *div* $15 = 4$*,* $u_1 = 1 - 4 \cdot 0 = 1$*,* $v_1 = 0 - 4 \cdot 1 = -4$*,* $i = 2$*,* $r_2 = 15$ *mód* $9 = 6$*.*

i	r	c	u	v
-1	69		1	0
0	15		0	1
1	9	4	1	-4
2	6			

También ahora $r_i \neq 0$*. Entonces* $c_2 = 15$ *div* $9 = 1$*,* $u_2 = 0 - 1 \cdot 1 = -1$*,* $v_2 = 1 - 1 \cdot (-4) = 5$*,* i_3*,* $r_3 = 9$ *mód* $6 = 3$*.*

i	r	c	u	v
-1	69		1	0
0	15		0	1
1	9	4	1	-4
2	6	1	-1	5
3	3			

$r_3 \neq 0$*. Por tanto, actualizamos:* $c_3 = 9$ *div* $6 = 1$*,* $u_3 = 1 - 1 \cdot (-1) = 2$*,* $v_3 = -4 - 1 \cdot 5 = -9$*,* $i = 4$*,* $r_4 = 0$*.*

i	r	c	u	v
-1	69		1	0
0	15		0	1
1	9	4	1	-4
2	6	1	-1	5
3	3	1	2	-9
4	0			

Y ahora, como $r_i = 0$ *terminamos. El resultado es que* $d = 3$*,* $u = 2$ *y* $v = -9$*.*

Notemos como $3 = 69 \cdot 2 + 15 \cdot (-9)$*.*

Una consecuencia inmediata del teorema 2.3.2 es el siguiente corolario:

Corolario 2.3.2. *Sean* $a, b \in \mathbb{Z}$*. Entonces existen números enteros* u *y* v *tales que* $1 = a \cdot u + b \cdot v$ *si, y sólo si,* $mcd(a, b) = 1$*.*

Demostración: El teorema de Bezout nos dice que si $mcd(a, b) = 1$ entonces existen $u, v \in \mathbb{Z}$ satisfaciendo la igualdad deseada.

Recíprocamente, supongamos que tenemos $u, v \in \mathbb{Z}$ tales que $1 = au + bv$. Sea ahora d un divisor común de a y b. Entonces:

$$\left.\begin{array}{rcl} d|a & \Longrightarrow & d|au \\ d|b & \Longrightarrow & d|bv \end{array}\right\} \Longrightarrow d|(au + bv) \Longrightarrow d|1$$

De donde se deduce que $mcd(a, b) = 1$. ■

Dos números cuyo máximo común divisor vale 1 se dice que son primos relativos.

Corolario 2.3.3. *Sean $a, m, n \in \mathbb{Z}$. Entonces $mcd(a, mn) = 1$ si, y sólo si, $mcd(a, m) = mcd(a, n) = 1$.*

Demostración: Si $mcd(a, mn) = 1$ existen $u, v \in \mathbb{Z}$ tales que $1 = au + mnv$. Agrupando de manera apropiada tenemos que $1 = au + m(nv)$ y $1 = au + n(mv)$, luego $mcd(a, m) = mcd(a, n) = 1$.

Recíprocamente, supongamos que $mcd(a, m) = mcd(a, n) = 1$. Existen entonces $u_m, v_m, u_n, v_n \in \mathbb{Z}$ tales que $1 = au_m + mv_m$ y $1 = au_n + nv_n$, luego

$$1 = au_m + mv_m(au_n + nv_n) = a(u_m + mv_m u_n) + mn(v_m v_n)$$

lo que nos dice que $mcd(a, mn) = 1$. ■

Corolario 2.3.4. *Sean $a, b, c \in \mathbb{Z}$. Si $a|(bc)$ y $mcd(a, b) = 1$ entonces $a|c$.*

Demostración: Sabemos, por el corolario anterior que existen $u, v \in \mathbb{Z}$ tal que $au + bv = 1$, y existe x tal que $bc = ax$. Entonces:

$$c = c(au + bv) = cau + cbv = cau + axv = a(cu + xv)$$

de donde se deduce que c es múltiplo de a. ■

Utilizaremos este corolario para demostrar que dos números cualesquiera tienen también mínimo común múltiplo.

Lema 2.3.2. *Sean $a, b \in \mathbb{Z}$. Si $mcd(a, b) = 1$ entonces ab es un mínimo común múltiplo de a y b.*

Demostración: Claramente ab es múltiplo común de a y b.

Supongamos ahora que $a|n$ y $b|n$. Entonces $n = bc$, luego $a|bc$, y por el corolario anterior $a|c$, lo que implica que $c = ax$. Por tanto, $n = abx$, de donde se deduce que $ab|n$. ■

Proposición 2.3.1. *Sean $a, b \in \mathbb{N}$ y $d = mcd(a, b)$. Entonces $mcm(a, b) = \frac{ab}{d}$.*

Demostración: Sean $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$. Entonces $mcd(a', b') = 1$, luego $mcm(a', b') = a'b'$.

Se tiene entonces que $mcm(a'd, b'd) = a'b'd$, o lo que es lo mismo

$$mcm(a, b) = \frac{ab}{d}$$

■

Nótese que $mcd(a, b) \cdot mcm(a, b) = ab$.

Ejemplo 2.3.7. *Sabemos que $mcd(4, 6) = 2$. Por tanto, $mcm(4, 6) = \frac{24}{2} = 12$.*

Sabemos que $mcd(1005, 450) = 15$. Entonces $mcm(1005, 450) = 1005 \cdot 30 = 30150$.

2.4. Números primos. Teorema fundamental de la aritmética

En esta sección vamos a demostrar el conocido teorema fundamental de la aritmética, que afirma que todo número natural mayor o igual que 2 se expresa de forma única como producto de números primos.

Comenzamos definiendo los números irreducibles.

Definición 40. *Sea p un número entero distinto de 0, 1 y -1. Se dice que p es irreducible si sus únicos divisores son ± 1 y $\pm p$.*

Ejemplo 2.4.1. *Son irreducibles 2, 3, 5.*

No es irreducible 4, pues 2 es un divisor suyo.

Claramente, si p es irreducible también lo es $-p$.

Veamos a continuación una caracterización de los números irreducibles.

Proposición 2.4.1. *Sea p un número entero distinto de 0, 1 y -1. Entonces:*

$$p \text{ es irreducible} \iff (p|ab \implies p|a \text{ ó } p|b)$$

Antes de hacer la demostración veamos algún ejemplo.

Ejemplo 2.4.2. *Sabemos que si el producto de dos números es par, al menos uno de ellos debe ser par. Puesto que ser par es equivalente a ser múltiplo de* 2*, lo que estamos diciendo es que*

$$2|ab \text{ implica } 2|a \text{ ó } 2|b$$

lo que de acuerdo con la proposición es decir que 2 *es irreducible (algo que ya sabíamos).*

De la misma forma, si el producto de dos números es múltiplo de 3*, uno de los factores debe serlo.*

Por otra parte, si tomamos $a = 8$ *y* $b = 15$*, entonces* $ab = 120$*, que es múltiplo de* 6*, mientras que ni* a *ni* b *lo son, luego la implicación*

$$6|ab \text{ implica } 6|a \text{ ó } 6|b$$

es falsa, pues hemos encontrado a *y* b *para los que se da la primera parte de la implicación, pero no la segunda. De acuerdo con la proposición esto nos diría que* 6 *no es irreducible.*

Vamos ya a la demostración.

Demostración: Hagamos en primer lugar la implicación hacia la izquierda. Es decir, suponemos que la implicación $p|ab \implies p|a$ ó $p|b$ es cierta y queremos probar que p es irreducible.

Sea d un divisor de p. Esto implica que $p = dx$, de donde $p|dx$. Pueden ocurrir dos cosas: que p divida a d o que p divida a x.

Si $p|d$, como $d|p$ entonces $d = \pm p$.

Si $p|x$ entonces $x = py$ para algún $y \in \mathbb{Z}$. Se tiene que $p = dx = dyp$, luego $dy = 1$ y por tanto $d = \pm 1$.

Por tanto, si d es un divisor de p entonces $d = \pm p$ o $d = \pm 1$, lo que dice que p es irreducible.

Veamos ahora la implicación hacia la derecha.

Supongamos que p es irreducible y que tenemos dos números enteros a y b tales que $p|ab$ (es decir, $ab = px$).

Puede ocurrir que p divida a a (en cuyo caso no hay nada que probar), o que p no divida a a. Veamos entonces que $p|b$.

Es claro que $mcd(p, a) = 1$. El corolario 2.3.4 nos dice que $p|b$, como queríamos.

■

Como es bien conocido, a los números irreducibles los llamaremos también números primos.

Como ejercicio, demuestra que si p es un número primo y tenemos $a_1, a_2, \cdots, a_n \in \mathbb{Z}$ tales que $p|(a_1 a_2 \cdots a_n)$ entonces existe $i \in \{1, 2, \cdots, n\}$ tal que $p|a_i$.

Estamos ya en condiciones de dar el teorema fundamental de la aritmética.

Teorema 2.4.1 (Teorema fundamental de la aritmética)**.** *Sea* $a \in \mathbb{N}$*,* $a \geq 2$*. Entonces,* a *es primo, o* a *se expresa de forma única (salvo el orden y el signo) como producto de números primos.*

Observación:

Sea $a = 6$. Sabemos que a lo podemos poner como producto de primos de la forma $6 = 2 \cdot 3$. Pero también podemos ponerlo como $6 = (-2) \cdot (-3)$. Aunque estrictamente hablando estas dos factorizaciones son distintas, ambas podrían considerarse iguales. De ahí que digamos que la factorización es única salvo el signo. De la misma forma, las factorizaciones $6 = 2 \cdot 3 = 3 \cdot 2$ son iguales salvo el orden.

Demostración: Para demostrar esto, veremos en primer lugar que todo número mayor que 1 tiene un divisor primo.

Sea a un número natural mayor o igual que 2. Llamaremos a este número b_0. Si b_0 es primo, entonces b_0 es un divisor primo de a. En caso de que no sea primo, tendrá un divisor positivo que no es ni 1 ni b_0. Sea este b_1. Es claro que $b_1 < b_0$.

Si b_1 es primo, ya tenemos un divisor primo de a. De no serlo, tendrá un divisor, b_2 que será menor que b_1 (y mayor que 1).

Obtenemos de esta forma una sucesión estrictamente decreciente $b_0, b_1, \cdots$ Como la sucesión no puede ser infinita, tendrá un término b_k que será un número primo. Pues este número es un divisor primo de a.

Sea ahora a un número mayor que 1. Si a es primo, ya tenemos a como producto de números primos (habría sólo un factor). Si no es primo, tendrá un divisor primo. Sea este p_1. Entonces $a = p_1 \cdot c_1$. Claramente $c_1 < a$.

Si c_1 es primo, ya tenemos a como producto de primos. Si no lo es, tomamos un divisor primo de c_1 (llamémoslo p_2, y tendremos que $c_1 = p_2 \cdot c_2$, luego $a = p_1 \cdot p_2 \cdot c_2$.

Tenemos de esta forma una sucesión $c_1, c_2, \cdots$ estrictamente decreciente. Por tanto, algún término c_k será el último, lo que significará que c_k es primo. En tal caso, tendremos escrito a como producto de números primos.

Veamos ahora la unicidad.

Sea a un número natural, y supongamos que tenemos dos factorizaciones de a como producto de primos: $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$.

Entonces se tiene que $p_1 | (q_1 \cdots q_s)$, y por ser p_1 primo, debe existir algún i tal que $p_1 | q_i$. Reordenamos los primos $q_1, \cdots, q_s$ para que el primo al que divida p_1 sea el primero (es decir, $p_1 | q_1$). Como q_1 es primo, entonces $p_1 = q_1$. Tenemos entonces que $\frac{a}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s$.

Repetimos ahora el mismo razonamiento, y llegamos (después de reordenar los primos) a que $p_2 = q_2$.

Continuando con este proceso, tendremos que $p_3 = q_3$, etc. Y así, los primos que aparecen en la primera factorización de a son los mismo que aparecen en la segunda. ■

Ejemplo 2.4.3. *Sea* $a = 6120$. *Claramente no es primo. Un divisor primo suyo es* 2. *Dividimos por 2, y tenemos que* $a = 2 \cdot 3060$.

Como 3060 *no es primo, buscamos un divisor primo suyo, que podría volver a ser 2. Tenemos* $3060 = 2 \cdot 1530$.

Este número vuelve a no ser primo y a tener a 2 como divisor primo suyo. $1530 = 2 \cdot 765$.

Este número no es primo, pero ahora 2 no es divisor suyo. Sí lo es 3. Entonces $765 = 3 \cdot 255$.

El 3 vuelve a ser un divisor primo. Dividimos por 3: $255 = 3 \cdot 85$.

El 5 es un divisor primo de 85. El cociente sale 17. Y este número ya es primo.

Si vemos la sucesión c_i *que hemos ido obteniendo ha sido* $c_1 = 3060$, $c_2 = 1530$, $c_3 = 765$, $c_4 = 255$, $c_5 = 85$, $c_6 = 17$. *Es una sucesión estrictamente decreciente y que acaba en un número primo.*

La factorización de 6120 como producto de primos es $6120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 17 = 2^3 \cdot 3^2 \cdot 5 \cdot 17$.

La factorización de un número como producto de primos permite de forma fácil determinar los divisores de un número. Así, si $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ y $b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ entonces $b|a$ si, y sólo si, $f_i \leq e_i$.

De esta forma es fácil comprobar que el conjunto

$$D(a) = \{p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r} : 0 \leq f_i \leq e_i\}$$

es el conjunto de todos los divisores positivos de a.

El cardinal de dicho conjunto es $(e_1 + 1) \cdot (e_2 + 1) \cdots (e_r + 1) = \prod_{k=1}^{r} (e_k + 1)$.

Ejemplo 2.4.4. *Sea* $a = 180$. *Entonces* $a = 2^2 3^2 5$. *Los divisores de a son entonces:*

$2^0 3^0 5^0 = 1$	$2^0 3^0 5^1 = 5$	$2^0 3^1 5^0 = 3$	$2^0 3^1 5^1 = 15$	$2^0 3^2 5^0 = 9$	$2^0 3^2 5^1 = 45$
$2^1 3^0 5^0 = 2$	$2^1 3^0 5^1 = 10$	$2^1 3^1 5^0 = 6$	$2^1 3^1 5^1 = 30$	$2^1 3^2 5^0 = 18$	$2^1 3^2 5^1 = 90$
$2^2 3^0 5^0 = 4$	$2^2 3^0 5^1 = 20$	$2^2 3^1 5^0 = 12$	$2^2 3^1 5^1 = 60$	$2^2 3^2 5^0 = 36$	$2^2 3^2 5^1 = 180$

Es decir,

$$D(180) = \{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180\}$$

que vemos que tiene 18 *elementos (notemos que* $18 = (2 + 1) \cdot (2 + 1) \cdot (1 + 1)$*).*

También podemos calcular el máximo común divisor y el mínimo común múltiplo de dos números.

Proposición 2.4.2. *Sean* $a, b \in \mathbb{N}^*$. *Supongamos que* $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ *y* $b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ *son las factorizaciones de a y b como producto de irreducibles. Entonces:*

$$mcd(a, b) = p_1^{mín\{e_1, f_1\}} p_2^{mín\{e_2, f_2\}} \cdots p_r^{mín\{e_r, f_r\}}$$

$$mcm(a, b) = p_1^{máx\{e_1, f_1\}} p_2^{máx\{e_2, f_2\}} \cdots p_r^{máx\{e_r, f_r\}}$$

Esta proposición puede generalizarse fácilmente para el cálculo del máximo común divisor y/o el mínimo común múltiplo de 3 ó más números.

Ejemplo 2.4.5. *En el ejemplo 2.3.5 calculamos el máximo común divisor de 1005 y 450, mientras que en el ejemplo 2.3.7 calculamos su mínimo común múltiplo. Vamos a hacerlo ahora siguiendo la proposición que acabamos de ver.*

Para eso, factorizamos ambos números:

$1005 = 3 \cdot 5 \cdot 67$*;* $450 = 2 \cdot 3^2 \cdot 5^2$*. Por tanto, de acuerdo con esta proposición tenemos que:*

$mcd(1005, 450) = 2^0 \cdot 3^1 \cdot 5^1 \cdot 67^0 = 15$*, y* $mcm(1005, 450) = 2^1 \cdot 3^2 \cdot 5^2 \cdot 67^1 = 30150$

Que coinciden con los valores obtenidos previamente.

Sean $a = 350$ *y* $b = 1155$*. Entonces se tiene que* $a = 2 \cdot 5^2 \cdot 7$ *y* $b = 3 \cdot 5 \cdot 7 \cdot 11$*. Por tanto*

$$mcd(350, 1155) = 2^0 3^0 5^1 7^1 11^0 = 5 \cdot 7 = 35 \qquad mcm(350, 1155) = 2^1 3^1 5^2 7^1 11^1 = 11550$$

2.5. Clases residuales módulo m

En el capítulo anterior construimos, para cada número natural $m \geq 1$ el conjunto $\mathbb{Z}_m$. Este conjunto fue definido como el conjunto cociente de $\mathbb{Z}$ por la relación de equivalencia

$$a \equiv b(\text{mód } m) \text{ si } m|(b-a)$$

Vimos que el conjunto $\mathbb{Z}_m$ tiene exactamente m elementos. De hecho, podemos escribir $\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \cdots, [m-1]_m\}$ donde $[i]_m \in \mathbb{Z}_m$ representa a la clase de equivalencia del elemento i, que está formada por todos los números enteros que al dividir por m dan resto i.

Con la función *módulo* (ver definición 36) tenemos que $a \equiv b(\text{mód } m)$ si, y sólo si, $a \text{ mód } m = b \text{ mód } m$.

Vamos a continuación a estudiar la estructura algebraica de estos conjuntos. Para ello necesitamos el siguiente lema:

Lema 2.5.1. *Sean* $a, b, c, d \in \mathbb{Z}$ *y* $m \geq 2$*. Entonces:*

1. $\left.\begin{array}{l} a \equiv c(\text{mód } m) \\ b \equiv d(\text{mód } m) \end{array}\right\} \Longrightarrow a + b \equiv c + d(\text{mód } m)$

2. $\left.\begin{array}{l} a \equiv c(\text{mód } m) \\ b \equiv d(\text{mód } m) \end{array}\right\} \Longrightarrow ab \equiv cd(\text{mód } m)$

Demostración:

1. $$\left.\begin{array}{lll} a \equiv c(\text{mód } m) & \Longrightarrow & m|(c-a) \\ b \equiv d(\text{mód } m) & \Longrightarrow & m|(d-b) \end{array}\right\} \Longrightarrow m|(c-a+d-b) \Longrightarrow m|(c+d-(a+b))$$
$$\Longrightarrow a + b \equiv c + d(\text{mód } m)$$

2. $$\left.\begin{array}{lllll} a \equiv c(\text{mód } m) & \Longrightarrow & m|(c-a) & \Longrightarrow & m|(c-a)b \\ b \equiv d(\text{mód } m) & \Longrightarrow & m|(d-b) & \Longrightarrow & m|c(d-b) \end{array}\right\} \Longrightarrow m|[c(d-b)+(c-a)b]$$
$$\Longrightarrow m|(cd-ab)$$
$$\Longrightarrow ab \equiv cd(\text{mód } m)$$

■

Nótese que a partir de este lema se tiene que si $[a]_m = [c]_m$, y $[b]_m = [d]_m$ entonces $[a+b]_m = [c+d]_m$ y $[ab]_m = [cd]_m$. Esto da pie a la siguiente definición.

Definición 41. *Sean* $a, b \in \mathbb{Z}$ *y* $m \geq 2$*. Se definen en* $\mathbb{Z}_m$ *las operaciones:*

$$[a]_m + [b]_m = [a+b]_m \qquad [a]_m[b]_m = [ab]_m$$

El lema anterior nos asegura que estas definiciones no dependen de los representantes que se elijan para $[a]_m$ y $[b]_m$.

Ejemplo 2.5.1. *Sea* $m = 9$*. En* $\mathbb{Z}_m$ *se tiene que* $[5] + [7] = [12] = [3]$*. Si en lugar de* $[5]$ *tomamos* $[23]$*, y en lugar de* $[7]$ *tomamos* $[34]$ *se tiene que* $[23] + [34] = [57] = [3]$ *(pues* $57 - 3 = 9 \cdot 6$*). Vemos como la elección del representante del primer sumando (*5 *ó* 23*) así como la elección del representante del segundo sumando (*7 *ó* 34*) no influye en el resultado final de la suma.*

De la misma forma, $[5]\cdot[7]=[35]=[8]$*, mientras que* $[23]\cdot[34]=[782]=[8]$.

Supongamos que tenemos dos números enteros a,b *tales que* $b|a$*,* $m\geq 2$ *y quisiéramos definir* $\frac{[a]_m}{[b]_m}$ *como sigue:*

$$\frac{[a]_m}{[b]_m}=\left[\frac{a}{b}\right]_m$$

Tomamos $m=8$*,* $a=6$ *y* $b=2$*. Entonces tendríamos que* $\frac{[6]}{[2]}=[3]$*. Ahora bien,* $[6]_8=[14]_8$*, mientras que* $\frac{[14]}{[2]}=[7]$*, y claramente* $[3]\neq[7]$ *en* $\mathbb{Z}_8$*. Es decir, el resultado final depende de los representantes elegidos. Esta operación, por tanto, no está bien definida.*

Nota: A partir de ahora, dado $a\in\mathbb{Z}$, denotaremos por a al elemento $[a]_m\in\mathbb{Z}_m$. En cada momento deberá quedar claro si a representa un número entero o un elemento de $\mathbb{Z}_m$. Así, se tiene que

$$\mathbb{Z}_m=\{0,1,2,\cdots,m-1\}$$

e igualdades como $4+6=3$, $5=1$ ó $9=0$ tendrán sentido en un contexto apropiado (la primera igualdad es válida en $\mathbb{Z}_7$, la segunda en $\mathbb{Z}_4$ o $\mathbb{Z}_2$ y la tercera en $\mathbb{Z}_9$ o $\mathbb{Z}_3$).

Proposición 2.5.1. *Sea* $m\geq 2$*. Las operaciones suma y producto verifican las siguientes propiedades:*

i) $a+(b+c)=(a+b)+c$

ii) $a+b=b+a$

iii) $a+0=a$

iv) Para cada $a\in\mathbb{Z}_m$ *existe* $b\in\mathbb{Z}_m$ *tal que* $a+b=0$.

v) $a(bc)=(ab)c$

vi) $ab=ba$

vii) $a1=a$

viii) $a(b+c)=ab+ac$

Estas propiedades nos dicen que $\mathbb{Z}_m$ es un anillo conmutativo.

Nótese que en general, el producto no tiene la propiedad cancelativa. Así, por ejemplo, en $\mathbb{Z}_8$ se verifica que $6\cdot 1=6\cdot 5$, y sin embargo $1\neq 5$.

Ejemplo 2.5.2. *Veamos las tablas de suma y producto en* $\mathbb{Z}_5$ *y* $\mathbb{Z}_6$*.*

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Definición 42. *Sea* $a\in\mathbb{Z}_m$*. Se dice que* a *es una unidad si existe* $b\in\mathbb{Z}_m$ *tal que* $a\cdot b=1$.

Ejemplo 2.5.3.

1. *Para cualquier $m \geq 2$, 1 es una unidad en $\mathbb{Z}_m$.*

2. *El elemento $3 \in \mathbb{Z}_5$ es una unidad (pues $3 \cdot 2 = 1$), mientras que $3 \in \mathbb{Z}_6$ no es unidad. Puede verse como en $\mathbb{Z}_5$ todo elemento distinto de cero es una unidad.*

Si $a \in \mathbb{Z}_m$ es una unidad, entonces se puede simplificar por a (es decir, $ab = ac \Longrightarrow b = c$). Razona el por qué.

Como consecuencia de lo anterior, si a es una unidad en $\mathbb{Z}_m$, hay un único elemento en $\mathbb{Z}_m$ que al multiplicarlo por él da 1. Este elemento se llama *inverso de a* y se representa por a^{-1}.

Denotaremos por $\mathcal{U}(\mathbb{Z}_m)$ al conjunto de todas las unidades de $\mathbb{Z}_m$.

Si $a, b \in \mathcal{U}(\mathbb{Z}_m)$, entonces $ab \in \mathcal{U}(\mathbb{Z}_m)$, y $(ab)^{-1} = a^{-1}b^{-1}$.

Todo lo dicho sobre unidades se puede hacer extensivo a cualquier anillo conmutativo.

Ejemplo 2.5.4.

$\mathcal{U}(\mathbb{Z}_2) = \{1\}$ $\mathcal{U}(\mathbb{Z}_3) = \{1, 2\}$ $\mathcal{U}(\mathbb{Z}_5) = \{1, 2, 3, 4\}$ $\mathcal{U}(\mathbb{Z}_6) = \{1, 5\}$ $\mathcal{U}(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$

$\mathcal{U}(\mathbb{Z}) = \{1, -1\}$ $\mathcal{U}(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$

Los inversos de las unidades en $\mathbb{Z}_9$ son $1^{-1} = 1$, $2^{-1} = 5$, $4^{-1} = 7$, $5^{-1} = 2$, $7^{-1} = 4$ y $8^{-1} = 8$. Observa como, por ejemplo, $4 \cdot 5 = 20 = 2$ es unidad, y $4^{-1} \cdot 5^{-1} = 7 \cdot 2 = 14 = 5 = 2^{-1}$.

Hemos calculado las unidades en algunos anillos $\mathbb{Z}_m$. Hasta ahora, la única forma de ver si un elemento en $\mathbb{Z}_m$ es unidad es multiplicarlo por los elementos de $\mathbb{Z}_m$ y comprobar si el algún caso de 1 ó no.

A la luz de los ejemplos anteriores vamos a comprobar la siguiente proposición.

Proposición 2.5.2. *Sea $a \in \mathbb{Z}_n$. Entonces a es unidad si, y sólo si, $mcd(a, n) = 1$.*

En el enunciado de esta proposición, las dos primeras veces que hablamos del elemento a hacemos referencia a un elemento de $\mathbb{Z}_n$, mientras que la tercera consideramos a como un número entero. En la demostración que vamos a hacer de esta proposición, también llamaremos de la misma forma a los elementos de $\mathbb{Z}_n$ y a los elementos de $\mathbb{Z}$. El contexto nos dirá cual de los dos casos se está considerando.

Nótese que decir $a = b$ (en $\mathbb{Z}_n$) es lo mismo que decir $b = a + kn$ (en $\mathbb{Z}$) para algún $k \in \mathbb{Z}$.

Puesto que $mcd(a, n) = mcd(a + kn, n)$, no influye para nada el representante que tomemos para comprobar, de acuerdo con la proposición precedente, si $a \in \mathbb{Z}_n$ es una unidad o no en $\mathbb{Z}_n$.

Demostración: Comprobemos la condición necesaria. Supongamos entonces que a es unidad en $\mathbb{Z}_n$. Sea $u = a^{-1}$, lo que nos dice que $au = 1$ (en $\mathbb{Z}_n$), o que $1 = au + kn$ (en $\mathbb{Z}$). El corolario 2.3.2 nos dice ahora que $mcd(a, n) = 1$.

En cuanto a la condición suficiente, suponemos que $mcd(a, n) = 1$. Existen entonces $u, v \in \mathbb{Z}$ tales que $au + nv = 1$. Vista esta igualdad en $\mathbb{Z}_n$ se tiene que $au = 1$ (pues $n = 0$), lo que nos dice que a es una unidad con inverso u. ■

La proposición anterior, junto con su demostración, aparte de darnos una condición necesesaria y suficiente para que un elemento de $\mathbb{Z}_n$ tenga inverso, nos da una forma de calcularlo. Basta hacer uso de la identidad de Bezout.

Ejemplo 2.5.5. *De la igualdad $1 = 11 \cdot 11 + 15 \cdot (-8)$ deducimos que 11 es una unidad en $\mathbb{Z}_{15}$ y que su inverso es 11.*

También deducimos que 15 es una unidad en $\mathbb{Z}_{11}$, y que su inverso es -8. Puesto que $15 = 4$ y $-8 = 3$ tenemos que 4 es unidad y $4^{-1} = 3$.

Basándonos en el algoritmo BEZOUT, vamos a dar un algoritmo que nos dirá si un elemento $a \in \mathbb{Z}_n$ tiene o no inverso, y en caso afirmativo, lo calculará.

Algoritmo INVERSO(a, n)

Entrada: $a, n \in \mathbb{Z}$, $n \geq 2$, $a \neq 0$.

Salida: $u :\ a \cdot u = 1$ en $\mathbb{Z}_n$ (si tal elemento existe).

$r_{-1} := a$, $r_0 := b$.

$v_{-1} := 0$, $v_0 := 1$.

$i := 1$.

$r_1 := r_{-1}$ mód r_0
Mientras $r_i \neq 0$
    $c_i := r_{i-2}$ div r_{i-1}.
    $v_i := v_{i-2} - v_{i-1} \cdot c_i$.
    $i := i + 1$.
    $r_i := r_{i-2}$ mód r_{i-1}.
Si $r_{i-1} \neq 1$
    Devuelve "No existe el inverso"
    Fin
Devuelve v_{i-1}.
Fin

Ejemplo 2.5.6. *Vamos a estudiar si* 391 *tiene inverso en* $\mathbb{Z}_{1542}$*, y en caso afirmativo vamos a calcularlo.*

r	c	v
1542		*0*
391		*1*
369	*3*	*-3*
22	*1*	*4*
17	*16*	*-67*
5	*1*	*71*
2	*3*	*-280*
1	*2*	*631*

Luego 391 *tiene inverso en* $\mathbb{Z}_{1542}$ *y éste vale* 631.

Antes de teminar la sección vamos a contar cuantas unidades tiene $\mathbb{Z}_n$. Para eso, introducimos la función φ de Euler.

Definición 43. *Sea* $m \geq 2$ *Se define* $\varphi(m)$ *como el número de elementos del conjunto* $\{0, 1, 2, \cdots, m-1\}$ *que son primos relativos con* m.

Nótese que $\varphi(m)$ es el cardinal del conjunto $\mathcal{U}(\mathbb{Z}_m)$
Tenemos entonces definida una aplicación $\varphi : \mathbb{N} \setminus \{0, 1\} \to \mathbb{N}$. Esta aplicación se conoce como la aplicación φ de Euler.

Ejemplo 2.5.7. *Vamos a dar los valores de* $\varphi(m)$ *para algunos números naturales.*
$\varphi(2) = 1$ *pues* $\mathcal{U}(\mathbb{Z}_2) = \{1\}$*. De la misma forma podemos ver que* $\varphi(3) = 2$*,* $\varphi(4) = 2$*,* $\varphi(5) = 4$*,* $\varphi(12) = 4$.
Si p *es un número primo, y* $1 \leq a \leq p - 1$ *se tiene que* $mcd(a, p) = 1$*. Por tanto,* $\varphi(p) = p - 1$.

Las dos siguientes propiedades son útiles a la hora de calcular el valor de $\varphi(m)$.

1. Si p es un número primo, entonces $\varphi(p^n) = p^n - p^{n-1}$.
2. Si $mcd(m, n) = 1$ entonces $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

La primera propiedad es fácil de justificar. Es fácil ver que $mcd(a, p^n) \neq 1$ si, y sólo si, $p|a$. Por tanto, los elementos del conjunto $\{1, 2, \cdots, p^n - 1, p^n\}$ que son primos relativos con p son exactamente los que no son múltiplos de p. Puesto que en $\{1, 2, \cdots, p^n - 1, p^n\}$ hay exactamente p^{n-1} múltiplos de p (los del conjunto $\{p \cdot 1, p \cdot 2, \cdots, p \cdot p^{n-1}\}$) deducimos que $\varphi(p^n) = p^n - p^{n-1}$.
La segunda propiedad la demostraremos más adelante.
Esta segunda propiedad se puede generalizar al siguiente caso:
Si $m_1, m_2, \cdots, m_k$ son números naturales tales que $mcd(m_i, m_j) = 1$ para $i \neq j$ entonces

$$\varphi(m_1 m_2 \cdots m_k) = \varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_k)$$

Ejemplo 2.5.8.

1. *Puesto que* $12 = 2^2 3$ *se tiene que*

$$\varphi(12) = \varphi(2^2 3) = \varphi(2^2) \cdot \varphi(3) = (2^2 - 2) \cdot (3 - 1) = 4$$

En la siguiente tabla, vamos a indicar el máximo común divisor con 12 de cada uno de los números comprendidos entre 0 *y* 11.

a	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
mcd(a,12)	*12*	*1*	*2*	*3*	*4*	*1*	*6*	*1*	*4*	*3*	*2*	*1*

y vemos que efectivamente hay cuatro números menores que 12 que son primos relativos con 12.

2. $30 = 2 \cdot 3 \cdot 5$, *luego* $\varphi(30) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) = (2-1)(3-1)(5-1) = 8$.
El conjunto de las unidades de $\mathbb{Z}_{30}$ *es* $\mathcal{U}(\mathbb{Z}_{30}) = \{1, 7, 11, 13, 17, 19, 23, 29\}$, *que vemos que tiene 8 elementos.*

3. *Si* $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ *donde todos los primos que intervienen son distintos, y todos los exponentes son mayores que* 0 *entonces:*

$$\varphi(m) = \varphi(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r}) = (p_1^{e_1} - p_1^{e_1 - 1})(p_2^{e_2} - p_2^{e_2 - 1}) \cdots (p_r^{e_r} - p_r^{e_r - 1})$$

o si queremos expresarlo de otra forma,

$$\varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Teorema 2.5.1 (Euler-Fermat)**.** *Sea* $a \in \mathbb{Z}$, $m \in \mathbb{N}^*$ *tales que* $mcd(a, m) = 1$. *Entonces* $a^{\varphi(m)} \equiv 1 (mód\ m)$.

Demostración: Nótese que decir $mcd(a, m) = 1$ es equivalente a decir que $a \in \mathcal{U}(\mathbb{Z}_m)$, luego hemos de probar que si $a \in \mathcal{U}(\mathbb{Z}_m)$ entonces $a^{\varphi(m)} = 1$ (en $\mathbb{Z}_m$).

Consideramos la aplicación $f : \mathcal{U}(\mathbb{Z}_m) \to \mathcal{U}(\mathbb{Z}_m)$ dada por $f(x) = a \cdot x$. Claramente f es inyectiva, pues al ser a una unidad se puede simplificar por a. Por tanto, f es sobreyectiva (pues va de un conjunto finito en sí mismo).

Si $\mathcal{U}(\mathbb{Z}_m) = \{x_1, x_2, \cdots, x_{\varphi(m)}\}$ entonces se tiene que

$$\mathcal{U}(\mathbb{Z}_m) = Im(f) = \{a \cdot x_1, a \cdot x_2, \cdots, a \cdot x_{\varphi(m)}\}$$

Por tanto, $x_1 x_2 \cdots x_{\varphi(m)} = (ax_1)(ax_2) \cdots (ax_{\varphi(m)}) = a^{\varphi(m)} x_1 x_2 \cdots x_{\varphi(m)}$, y puesto que todo lo que interviene en el producto son unidades podemos simplificar y nos queda $a^{\varphi(m)} = 1$. ■

Ejemplo 2.5.9.

1. *Se tiene que* $\varphi(5) = 4$. *Por tanto* $2^4 \equiv 1 (mód\ 5)$.
El conjunto de las unidades de $\mathbb{Z}_5$ *es* $\{1, 2, 3, 4\}$. *La aplicación* $f : \mathcal{U}(\mathbb{Z}_5) \to \mathcal{U}(\mathbb{Z}_5)$ *es la aplicación:*

$$1 \mapsto 2 \qquad 2 \mapsto 4 \qquad 3 \mapsto 1 \qquad 4 \mapsto 3$$

y vemos como es biyectiva.

2. $\varphi(7) = 6$ *luego* $3^6 \equiv 1 (mód\ 7)$, *o* $4^6 \equiv 1 (mód\ 7)$.

3. *Vamos a calcular el resto de dividir* 3^{1000} *y* 4^{1000} *entre* 7. *Es decir, vamos a calcular el valor de* 3^{1000} *y* 4^{1000} *en* $\mathbb{Z}_7$.
Sabemos que $3^6 = 1$, *y como* $1000 = 166 \cdot 6 + 4$ *tenemos que*

$$3^{1000} = 3^{6 \cdot 166} 3^4 = (3^6)^{166} 3^4 = 1^{166} 3^4 = 3^4 = 81 = 4$$

$$4^{1000} = 4^{6 \cdot 166} 4^4 = (4^6)^{166} 4^4 = 1^{166} 4^4 = (4^2)^2 = 2^2 = 4$$

Nótese que en este caso se tiene que $4^3 = 1$, *luego se podría haber hecho*

$$4^{1000} = 4^{3 \cdot 333} 4^1 = (4^3)^{333} 4 = 1^{166} 4 = 4$$

Si calculamos 3^{1000} *nos sale que vale*

$$1322070819480806636890455259752144365965422032752148167664920368226828597346704899540778313850608061963909777696872582355950954582100618911865342725257953674027620225198320803878014774228964841274390400117588618041128947815623094438061566173054086674490506178125480344405547054397038895817465368254916136220830268563778582290228416398307887896918556404084989376093732421718463599386955167650189405881090604260896714388641028143503856487471658320106143661321731027689028552200001$$

El cociente al dividir por 7 sale

$$1888672599258295195557793228217349094236317189645925953807029097466897996209578427915397591215154374234156825281246546222787077974429455588379061036082790962896600321711886862682878248898521201820557714453698025773041354022318706340087951675791552392129294540179257634865067220567198422596379097507023051744043240805397974700326309140439839852740794862978427053727676060245949799124221668071699151258700863229852449126630040205005509267816654743008776659031044325270040788857 1$$

mientras que el resto sale 4.

2.6. Sistemas de congruencias

En esta sección vamos a plantearnos resolver algunas ecuaciones, o sistemas de ecuaciones, con una incógnita, en donde esta incógnita aparece en una o varias congruencias. Las soluciones, de existir, serán números enteros.

Una ecuación lineal en congruencias es una expresión de la forma

$$ax + b \equiv cx + d(\text{mód } m)$$

donde a, b, c, d, m son números enteros y $m \neq 0$.

Por ejemplo, $3x + 4 \equiv -2x + 5(\text{mód } 12)$ es una ecuación lineal en congruencias. En este caso, $a = 3$, $b = 4$, $c = -2$, $d = 5$ y $m = 12$.

A una ecuación lineal en congruencias de la forma anterior la llamaremos simplemente una *congruencia.*

Dada una congruencia de la forma $ax + b \equiv cx + d(\text{mód } m)$, una solución de esta congruencia es un número entero, de forma que al sustituir x por ese número entero nos queda una afirmación cierta. Si s es una solución, normalmente escribiremos que $x = s$ es una solución de la congruencia.

Por ejemplo, en la congruencia $3x + 4 \equiv -2x + 5(\text{mód } 12)$, $x = 5$ es una solución, ya que al sustituir x por 5 nos queda $3 \cdot 5 + 4 \equiv -2 \cdot 5 + 5(\text{mód } 12)$, o lo que es lo mismo, $19 \equiv -5(\text{mód } 12)$, lo cual es cierto, pues 12 es un divisor de $-5 - 19$. También es solución $x = -7$. Sin embargo, no es solución $x = 7$, ya que si sustituimos x por 7, nos queda $21 \equiv -11(\text{mód } 12)$, y esa afirmación es falsa, ya que -32 (que es igual a $-11 - 21$) no es múltiplo de 12.

Nosotros no vamos a estudiar ecuaciones en congruencias que no sean lineales. El caso más simple es la congruencia

$$x \equiv a(\text{mód } m)$$

con $a, m \in \mathbb{Z}$, $m \geq 1$. Esta ecuación claramente tiene solución. De hecho, tiene infinitas soluciones y éstas son $x = a + km : \ k \in \mathbb{Z}$.

Por ejemplo, la congruencia $x \equiv 2(\text{mód } 5)$ tiene a $x = 2$ como solución, pero también $x = 7$, $x = 12$, $x = -3$. Todas las soluciones son de la forma $x = 2 + 5k$, con k un número entero. Para $k = 0, 1, 2, -1$ obtenemos las cuatro soluciones que hemos dado.

Dadas dos ecuaciones en congruencias, diremos que son equivalentes si ambas tienen las mismas soluciones.

Dados $a, b, c, d, m \in \mathbb{Z}$, $m \neq 0$, es fácil ver que la congruencia $ax + b \equiv cx + d(\text{mód } m)$ es equivalente a la congruencia $(a - c)x \equiv d - b(\text{mód } m)$, por lo que nos limitaremos a congruencias que sean de la forma $ax \equiv b(\text{mód } m)$

Por ejemplo, la congruencia $3x + 4 \equiv -2x + 5(\text{mód } 12)$ es equivalente a $(3 - (-2))x \equiv 5 - 4(\text{mód } 12)$, o lo que es lo mismo $5x \equiv 1(\text{mód } 12)$. Podemos ver como $x = 5$, ó $x = -7$ son soluciones de ambas, mientras que $x = 7$ no es solución de ninguna.

Nuestro primer objetivo es, dada una congruencia de la forma $ax \equiv b(\text{mód } m)$, estudiar si tiene o no solución, y en caso afirmativo, transformarla en una equivalente a ella que sea de la forma $x \equiv c(\text{mód } n)$. Una vez hecho esto, ya tenemos las soluciones de la congruencia de partida.

Veamos a continuación distintas transformaciones que podemos realizar en una congruencia, y que dan lugar a una congruencia equivalente. Supondremos que partimos de una congruencia de la forma $ax \equiv b(\text{mód } m)$

1. Si $a \equiv a'(\text{mód } m)$ y $b \equiv b'(\text{mód } m)$ entonces la congruencia $ax \equiv b(\text{mód } m)$ es equivalente a $a'x \equiv b'(\text{mód } m)$.

   Demostración: Se tiene que $a' = a + k_a m$, y $b' = b + k_b m$.

   Si x_0 es una solución de $ax \equiv b(\text{mód } m)$ entonces $ax_0 - b = km$, con $k \in \mathbb{Z}$. Entonces:

   $$\begin{aligned} a'x_0 - b' &= (a + k_a m)x_0 - (b + k_b m) = ax_0 + k_a m x_0 - b - k_b m = ax_0 - b + (k_a x_0 - k_b)m \\ &= km + (k_a x_0 - k_b)m = (k + k_a x_0 - k_b)m \end{aligned}$$

   es decir, $a'x_0 - b'$ es múltiplo de m, o lo que es lo mismo, x_0 es solución de $a'x \equiv b'(\text{mód } m)$

   Por tanto, hemos demostrado que toda solución de $ax \equiv b(\text{mód } m)$ es solución de $a'x \equiv b'(\text{mód } m)$

   De la misma forma se demuestra que toda solución de $a'x \equiv b'(\text{mód } m)$ es solución de $ax \equiv b(\text{mód } m)$ ■

   Esta propiedad nos permite, dada una congruencia, reducir los coeficientes módulo m, obteniendo una congruencia equivalente con coeficientes menores. Por ejemplo, la congruencia

   $$29x \equiv 67(\text{mód } 7)$$

   es equivalente a la congruencia

   $$x \equiv 4(\text{mód } 7)$$

   pues $29 \equiv 1(\text{mód } 7)$ y $67 \equiv 4(\text{mód } 7)$.

2. Si d es un divisor común de a, b y m, entonces la congruencia $\frac{a}{d}x \equiv \frac{b}{d}(\text{mód } \frac{m}{d})$ es equivalente a $ax \equiv b(\text{mód } m)$.

   Demostración: Sea x_0 una solución de $ax \equiv b(\text{mód } m)$. Entonces $ax_0 - b = km$, luego $\frac{a}{d}x_0 - \frac{b}{d} = k\frac{m}{d}$, luego x_0 es solución de $\frac{a}{d}x \equiv \frac{b}{d}(\text{mód } \frac{m}{d})$

   La otra parte se demuestra de forma análoga. ■

   Esta propiedad también permite reducir los coeficientes de las congruencias. Así, por ejemplo, las congruencias

   $$6x \equiv 14(\text{mód } 22) \quad \text{y} \quad 3x \equiv 7(\text{mód } 11)$$

   son equivalentes.

3. Si $mcd(c, m) = 1$, entonces las congruencias $ax \equiv b(\text{mód } m)$ y $cax \equiv cb(\text{mód } m)$ son equivalentes.

   Demostración: Es fácil comprobar que toda solución de $ax \equiv b(\text{mód } m)$ es también solución de $cax \equiv cb(\text{mód } m)$ (si $ax_0 - b$ es múltiplo de m también lo es $cax_0 - cb$). Esto es cierto, aún sin que $mcd(c, m) = 1$.

   Sea ahora d tal que $dc \equiv 1(\text{mód } m)$. Este tal d existe. Basta tomar el inverso de c en $\mathbb{Z}_m$, que existe pues $mcd(c, m) = 1$. Se tiene ahora que toda solución de $cax \equiv cb(\text{mód } m)$ es solución de $dcax \equiv dcb(\text{mód } m)$, que tiene las mismas soluciones que $ax \equiv b(\text{mód } m)$ (ver propiedad 1). ■

   Esta propiedad se suele aplicar junto con la propiedad 1, para simplificar congruencias. Por ejemplo, si tenemos la congruencia

   $$6x \equiv 16(\text{mód } 17)$$

   podemos multiplicar por 3 los coeficientes a y b, ya que $mcd(3, 17) = 1$. Obtenemos entonces la congruencia

   $$18x \equiv 48(\text{mód } 17)$$

   que es equivalente a la de partida. Por la propiedad primera, tenemos que esta congruencia es equivalente a

   $$x \equiv 14(\text{mód } 17)$$

   y de esta congruencia conocemos las soluciones.

   El número 3 por el que se ha multiplicado no ha sido elegido al azar, sino que se ha tomado por ser el inverso de 6 en $\mathbb{Z}_{17}$.

Parece claro entonces que el camino a seguir es multiplicar los coeficientes a y b de la congruencia por el inverso de a en $\mathbb{Z}_m$. El problema es que no siempre es posible.

Es importante que el número por el que multiplicamos sea primo relativo con m, pues en caso contrario obtenemos una congruencia que no es equivalente. Por ejemplo, si consideramos la congruencia

$$7x \equiv 5(\text{mód } 12)$$

y multiplicamos por 2, obtenemos

$$14x \equiv 10(\text{mód } 12)$$

Vemos como $x = 5$ es solución de la segunda congruencia ($14 \cdot 5 - 10$ es múltiplo de 12), pero no es solución de la primera ($7 \cdot 5 - 5$ no es múltiplo de 12).

4. Si c es un divisor común de a y b, y $mcd(c, m) = 1$, entonces las congruencias $ax \equiv b(\text{mód } m)$ y $\frac{a}{c}x \equiv \frac{b}{c}(\text{mód } m)$ son equivalentes.

   Demostración: Es semejante a la propiedad anterior. ■

Proposición 2.6.1. *Sean $a, b, m \in \mathbb{Z}$, con $m \geq 2$. Entonces la congruencia $ax \equiv b(\text{mód } m)$ tiene solución si, y sólo si, $mcd(a, m)|b$.*

Demostración: Sea $d = mcd(a, m)$.

Supongamos que la congruencia tiene solución. Sea x_0 una tal solución. Entonces $ax_0 - b = km$ para algún $k \in \mathbb{Z}$, luego $ax_0 - km = b$.

Puesto que a es múltiplo de d, también lo es ax_0. De la misma forma, km es múltiplo de d. Por tanto, $ax_0 - km$ es múltiplo de d. Es decir, $d|b$.

Recíprocamente, supongamos que $d|b$, es decir, $b = c \cdot d$ para algún $c \in \mathbb{Z}$. Por el teorema 2.3.2, existen $u, v \in \mathbb{Z}$ tales que $d = a \cdot u + m \cdot v$. Multiplicamos por c, y nos queda $b = a \cdot (uc) + m \cdot (vc)$, de donde deducimos que $a \cdot (uc) - b$ es múltiplo de m. Por tanto, uc es una solución a la congruencia $ax \equiv b(\text{mód } m)$. ■

A la hora de resolver una congruencia de la forma $ax \equiv b(\text{mód } m)$ podemos proceder como sigue:

- Reducimos a y b módulo m. Este paso no es necesario, pero puede facilitar los cálculos.
- Se comprueba si $mcd(a, m)|b$. Si la respuesta es negativa, entonces la congruencia no tiene solución. Si la respuesta es afirmativa, podemos dividir toda la congruencia por $mcd(a, m)$ (ver propiedad 2).

  Hemos transformado la congruencia en una de la forma $ax \equiv b(\text{mód } m)$, pero ahora se tiene que $mcd(a, m) = 1$.
- Buscamos el inverso de a en $\mathbb{Z}_m$. Llamémoslo u.
- Multiplicamos ambos miembros de la congruencia por u. Por la propiedad 3 obtenemos una congruencia equivalente, y ésta adopta la forma $x \equiv c(\text{mód } m)$.

Con esto ya hemos resuelto la congruencia. Las soluciones son $x = c + km : \ k \in \mathbb{Z}$.

Ejemplo 2.6.1.

1. *La congruencia $2x \equiv 3(\text{mód } 4)$ no tiene solución, pues $mcd(2, 4) = 2$, que no divide a 3. Claramente, para cualquier valor de x, $2x$ es par, luego $2x - 3$ es impar, y un número impar no puede ser múltiplo de 4.*

2. *En cambio, la congruencia $4x \equiv 2(\text{mód } 6)$ sí tiene solución, pues $mcd(4, 6) = 2$ y $2|2$. Dividimos entonces todo por 2 y obtenemos la congruencia $2x \equiv 1(\text{mód } 3)$. Puesto que $2^{-1} = 2$ (en $\mathbb{Z}_3$) la congruencia es equivalente a $x \equiv 2(\text{mód } 3)$, cuyas soluciones son $x = 2 + 3k$.*

3. *Vamos a resolver la congruencia $48x \equiv 25(\text{mód } 15)$. En primer lugar, reducimos módulo 15. La congruencia nos queda $3x \equiv 10(\text{mód } 15)$. Dado que $mcd(3, 15) = 3$, y éste no divide a 10 la congruencia no tiene solución.*

4. *Resolvamos ahora* $27x \equiv 13(mód\ 10)$.

   Reducimos todos los coeficientes módulo 10.

   $$7x \equiv 3(mód\ 10)$$

   Puesto que $mcd(7, 10) = 1$ *la congruencia tiene solución.*

   $7^{-1} = 3$. *Multiplicamos entonces por* 3.

   $$x \equiv 9(mód\ 10)$$

   Las soluciones son $x = 9 + 10k$.

5. *Consideramos la congruencia* $6x \equiv 12(mód\ 27)$. *Se tiene que* $x = 11$ *es solución de esta ecuación, pues* $6 \cdot 11 - 12 = 54$ *que es múltiplo de* 27.

   Si dividimos ambos miembros por 3 *obtenemos* $2x \equiv 4(mód\ 27)$. *En este caso tenemos que* 11 *no es solución, pues* $2 \cdot 11 - 4 = 18$ *que no es múltiplo de* 27.

6. *Obviamente, si partimos de la congruencia* $2x \equiv 4(mód\ 27)$ *y multiplicamos ambos miembros por* 3 *obtenemos una congruencia que no es equivalente.*

El siguiente algoritmo recoge esta forma de resolver una congruencia.

Algoritmo CONGRUENCIA(a, b, m)
Entrada: $a, b \in \mathbb{Z}, m \in \mathbb{N} : m \geq 1$
Salida: (c, n): $x \equiv c(\text{mód } n)$ y $ax \equiv b(\text{mód } m)$ son equivalentes.
    $a := a$ mód m
    $b := b$ mód m
    $(d, u, v) := BEZOUT(a, m)$
    Si b mód $d \neq 0$
        Devuelve "No tiene solución"
        Fin
    $(a, b, m) := (a \text{ div } d, m \text{ div } d, m \text{ div } d)$
    $c := a \cdot u$ mód m
    Devuelve (c, m)
    Fin

Nos planteamos a continuación cómo resolver sistemas de congruencias con una sola incógnita. Puesto que toda congruencia que tenga solución es equivalente a una de la forma $x \equiv a(\text{mód } m)$ nos planteamos resolver un sistema de la forma

$$\begin{aligned} x &\equiv a_1(\text{mód } m_1) \\ x &\equiv a_2(\text{mód } m_2) \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_p(\text{mód } m_p) \end{aligned}$$

Una solución del sistema es un número entero que es simultáneamente solución de todas las congruencia.

Ejemplo 2.6.2.

1. *El sistema de congruencias*

   $$x \equiv 2(mód\ 6)$$
   $$x \equiv 5(mód\ 9)$$

   tiene a $x = 14$ *como una solución, pues* $14 - 2$ *es múltiplo de* 6 *y* $14 - 5$ *es múltiplo de* 9.

2. *El sistema*

   $$x \equiv 2(mód\ 6)$$
   $$x \equiv 6(mód\ 9)$$

   no tiene solución, pues si $x \equiv 6(mód\ 9)$ *se tiene que* $x \equiv 0(mód\ 3)$, *mientras que si* $x \equiv 2(mód\ 6)$ *entonces* $x \equiv 2(mód\ 3)$.

El siguiente teorema nos da una condición suficiente para que un sistema de congruencias tenga solución.

Teorema 2.6.1 (Teorema chino del resto)**.** *Sean $a_1, a_2, \cdots, a_p \in \mathbb{Z}$, y $m_1, m_2, \cdots, m_p \in \mathbb{N}^*$. Supongamos que $mcd(m_i, m_j) = 1$ para $i \neq j$. Entonces el sistema de congruencias*

$$\begin{array}{c} x \equiv a_1 (mód\ m_1) \\ x \equiv a_2 (mód\ m_2) \\ \cdots\cdots\cdots\cdots \\ x \equiv a_p (mód\ m_p) \end{array}$$

tiene solución. Además, si a es una solución, dicho sistema es equivalente a la congruencia

$$x \equiv a (mód\ M)$$

donde $M = \prod_{i=1}^{p} m_i$.

Antes de hacer la demostración del teorema, comprueba que si $a, m_1, m_2, \cdots m_p \in \mathbb{Z}$ y $mcd(a, m_1) = mcd(a, m_2) = \cdots = mcd(a, m_p) = 1$ entonces $mcd(a, m_1 m_2 \cdots m_p) = 1$.

Demostración: Sea $M_i = \frac{M}{m_i} = \prod_{j \neq i} m_j$.

Se tiene entonces que $mcd(m_i, M_i) = 1$. Por el teorema 2.3.2, existen $u_i, v_i \in \mathbb{Z}$ tal que $m_i u_i + M_i v_i = 1$. Es claro entonces que

$$M_i v_i \text{ mód } m_i = 1 \qquad M_i v_i \text{ mód } m_j = 0 \ \text{ para } j \neq i$$

luego

$$a_i M_i v_i \text{ mód } m_i = a_i \text{ mód } m_i \qquad a_i M_i v_i \text{ mód } m_j = 0 \ \text{ para } j \neq i$$

Sea entonces $a = \sum_{i=1}^{p} a_i M_i v_i$. Es fácil comprobar que a es solución del sistema.

Supongamos que b es otra solución. Entonces se tiene que

$$b \equiv a (\text{mód } m_1) \quad b \equiv a (\text{mód } m_2) \quad \cdots \quad b \equiv a (\text{mód } m_p)$$

es decir,

$$m_1 | (b - a) \quad m_2 | (b - a) \quad \cdots \quad m_p | (b - a)$$

lo que es equivalente a que $mcm(m_1, m_2, \cdots, m_p) | (b - a)$. Y como $mcm(m_1, m_2, \cdots, m_p) = M$, lo que tenemos es que $M | (b - a)$, es decir, $b = a + Km$. Por tanto, todas las soluciones del sistema de congruencias son de la forma $a + Km$, las mismas soluciones que tiene la congruencia $x \equiv a (\text{mód } M)$. ■

Nótese que el teorema chino del resto, lo que nos dice es que la aplicación

$$f : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_p}$$

dada por

$$f(x) = (x \text{ mód } m_1, x \text{ mód } m_2, \cdots x \text{ mód } m_p)$$

es biyectiva (realmente, lo que dice es que es sobreyectiva, pero al tener los dos conjuntos el mismo cardinal eso es suficiente para ser biyectiva).

Nos centramos en el caso $p = 2$. Es fácil ver (corolario 2.3.3) que la aplicación f induce una biyección

$$f : \mathcal{U}(\mathbb{Z}_{m_1 m_2}) \to \mathcal{U}(\mathbb{Z}_{m_1}) \times \mathcal{U}(\mathbb{Z}_{m_2})$$

Por tanto, los dos conjuntos, dominio y codominio, tienen el mismo cardinal. Deducimos entonces que

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$$

si $mcd(m_1, m_2) = 1$.

Ejemplo 2.6.3.

1. *Consideramos el sistema:*

$$\begin{array}{l} x \equiv 1(\textit{mód } 2) \\ x \equiv 2(\textit{mód } 5) \\ x \equiv 3(\textit{mód } 7) \end{array}$$

Es claro que $mcd(2,5) = mcd(2,7) = mcd(5,7) = 1$. *Entonces tomamos* $M_1 = 5 \cdot 7 = 35$, $M_2 = 2 \cdot 7 = 14$ *y* $M_3 = 2 \cdot 5 = 10$.

$1 = 2 \cdot 18 + 35 \cdot (-1) \implies v_1 = -1$

$1 = 5 \cdot 3 + 14 \cdot (-1) \implies v_2 = -1$

$1 = 7 \cdot 3 + 10 \cdot (-2) \implies v_3 = -2$.

Por tanto, podemos tomar $a = 1 \cdot 35 \cdot (-1) + 2 \cdot 14 \cdot (-1) + 3 \cdot 10 \cdot (-2) = -123$.

El sistema de partida es equivalente a la congruencia $x \equiv -123(\textit{mód } 70)$, *que a su vez es equivalente a* $x \equiv 17(\textit{mód } 70)$. *Las soluciones son entonces*

$$x = 17 + 70k$$

Nótese que podríamos haber tomado $v_1 = 1$, $v_2 = 4$ *y* $v_3 = 5$, *en cuyo caso nos habría salido* $a = 297$, *que también es solución (*$297 \equiv -123(\textit{mód } 70)$*).*

2. *Consideramos la aplicación* $f : \mathbb{Z}_{18} \to \mathbb{Z}_2 \times \mathbb{Z}_9$ *dada por* $f(x) = (x \textit{ mód } 2, x \textit{ mód } 9)$.

$$\begin{array}{llllll} f(0) = (0,0) & f(1) = (1,1) & f(2) = (0,2) & f(3) = (1,3) & f(4) = (0,4) & f(5) = (1,5) \\ f(6) = (0,6) & f(7) = (1,7) & f(8) = (0,8) & f(9) = (1,0) & f(10) = (0,1) & f(11) = (1,2) \\ f(12) = (0,3) & f(13) = (1,4) & f(14) = (0,5) & f(15) = (1,6) & f(16) = (0,7) & f(17) = (1,8) \end{array}$$

que claramente es una biyección, mientras que si definimos $f : \mathbb{Z}_{18} \to \mathbb{Z}_3 \times \mathbb{Z}_6$ *de la misma forma obtenemos*

$$\begin{array}{llllll} f(0) = (0,0) & f(1) = (1,1) & f(2) = (2,2) & f(3) = (0,3) & f(4) = (1,4) & f(5) = (2,5) \\ f(6) = (0,0) & f(7) = (1,1) & f(8) = (2,2) & f(9) = (0,3) & f(10) = (1,4) & f(11) = (2,5) \\ f(12) = (0,0) & f(13) = (1,1) & f(14) = (2,2) & f(15) = (0,3) & f(16) = (1,4) & f(17) = (2,5) \end{array}$$

que claramente no es ni inyectiva ni sobreyectiva.

En un ejemplo anterior hemos estudiado dos sistemas con dos congruencias en los que los módulos no eran primos relativos ($mcd(m_1, m_2) \neq 1$). En un caso el sistema tiene solución y en el otro no. Lo que pretendemos a continuación es estudiar sistemas de congruencias que no se ajusten a las hipótesis del teorema chino del resto (que los módulos sean primos relativos).

Vamos a desarrollar un método para resolver sistemas de congruencias, independientemente de que satisfagan o no las hipótesis del teorema chino. En caso de que el sistema no tenga solución, lo detectaremos en el desarrollo del proceso.

El método consiste en resolver en primer lugar la primera congruencia (trivial).

Se introduce la solución en la segunda, y se halla la solución del sistema formado por las dos primeras congruencias.

Se introduce en la tercera congruencia y se vuelve a resolver.

El proceso continúa, bien hasta que terminemos con todas las congruencias, bien hasta que lleguemos a una congruencia que no tiene solución.

Veamos algunos ejemplos.

Ejemplo 2.6.4. *1.*

$$\left.\begin{array}{l} x \equiv 1(\textit{mód } 2) \\ x \equiv 2(\textit{mód } 5) \\ x \equiv 3(\textit{mód } 7) \end{array}\right\}$$

$x \equiv 1(mód\ 2)$	*Calculamos las soluciones*	$x = 1 + 2k_1$
$x \equiv 2(mód\ 5)$	*Introducimos la solución*	$1 + 2k_1 \equiv 2(mód\ 5)$
		$2k_1 \equiv 1(mód\ 5)$
	Multiplicamos por $3 = 2^{-1}$ *en* $\mathbb{Z}_5$	$k_1 \equiv 3(mód\ 5)$
		$k_1 = 3 + 5k_2$
	Sustituimos	$x = 1 + 2(3 + 5k_2) = 7 + 10k_2$
$x \equiv 5(mód\ 7)$	*Introducimos la solución*	$7 + 10k_2 \equiv 3(mód\ 7)$
		$10k_2 \equiv -4(mód\ 7)$
	Reducimos módulo 7	$3k_2 \equiv 3(mód\ 7)$
	Multiplicamos por $5 = 3^{-1}$ *en* $\mathbb{Z}_7$	$k_2 \equiv 1(mód\ 7)$
		$k_2 = 1 + 7k_2$
	Sustituimos	$x = 7 + 10(1 + 7k_2) = 17 + 70k_2$

Por tanto, la solución es $x = 17 + 70k_2$.

2. $\left.\begin{array}{l} x \equiv 2(mód\ 6) \\ x \equiv 5(mód\ 9) \end{array}\right\}$

$x \equiv 2(mód\ 6)$	*Calculamos las soluciones*	$x = 2 + 6k_1$
$x \equiv 5(mód\ 9)$	*Introducimos la solución*	$2 + 6k_1 \equiv 5(mód\ 9)$
		$6k_1 \equiv 3(mód\ 9)$
	Dividimos todo por $3 = mcd(6, 3, 9)$	$2k_1 \equiv 1(mód\ 3)$
	Multiplicamos por $2 = 2^{-1}$ *en* $\mathbb{Z}_3$	$k_1 \equiv 2(mód\ 3)$
		$k_1 = 2 + 3k_2$
	Sustituimos	$x = 2 + 6(2 + 3k_2) = 14 + 18k_2$

Las soluciones son entonces $x = 14 + 18k_2$.

3. $\left.\begin{array}{l} x \equiv 2(mód\ 6) \\ x \equiv 6(mód\ 9) \end{array}\right\}$

$x \equiv 2(mód\ 6)$	*Calculamos las soluciones*	$x = 2 + 6k_1$
$x \equiv 6(mód\ 9)$	*Introducimos la solución*	$2 + 6k_1 \equiv 6(mód\ 9)$
		$6k_1 \equiv 4(mód\ 9)$

Y el sistema no tiene solución, pues $mcd(6, 9) = 3$, *que no divide a* 4.

4. *Vamos a calcular las dos últimas cifras de* 27^{3636}.

Es claro que tenemos que calcular el resto de dividir por 100 *de dicho número, o lo que es equivalente, realizar la operación en* $\mathbb{Z}_{100}$. *Dado que* $mcd(27, 100) = 1$ *se tiene que* $27^{\varphi(100)} = 1$, *y como* $\varphi(100) = \varphi(4 \cdot 25) = 2 \cdot 20 = 40$ *tenemos que* $27^{40} \equiv 1(mód\ 100)$.

Puesto que $3636 = 90 \cdot 40 + 36$ *nos queda que* $27^{3636} = (27^{40})^{90}27^{36} = 27^{36}$. *Vemos que realizar esta operación no es fácil. Vamos a ver tres formas de resolverlo:*

a)
- *Calculamos* 27^{3636} *en* $\mathbb{Z}_4$.
  En ese caso se tiene que $27 = 3$, *y como* $\varphi(4) = 2$ *entonces* $3^2 = 1$, *luego* $3^{3636} = 1$.
- *Calculamos* 27^{3636} *en* $\mathbb{Z}_{25}$.
  En este caso hay que calcular 2^{3636}. *Dado que* $\varphi(25) = 20$ *y* $3636 \equiv 16(mód\ 20)$ *lo que hemos de calcular es* 2^{16}, *que puede ser calculado como sigue:*

$$2^2 = 4; \quad 2^4 = (2^2)^2 = 4^2 = 16; \quad 2^8 = (2^4)^2 = 16^2 = 256 = 6; \quad 2^{16} = (2^8)^2 = 6^2 = 36 = 11$$

- *Resolvemos el sistema*

$$\begin{array}{c} x \equiv 1(mód\ 4) \\ x \equiv 11(mód\ 25) \end{array}$$

$x = 1 + 4k_1$, *de donde* $1 + 4k_1 \equiv 11(mód\ 25)$, *es decir,* $4k_1 \equiv 10(mód\ 25)$. *Multiplicamos por* 19 *y nos queda* $k_1 \equiv 15(mód\ 25)$ *de donde* $k_1 = 15 + 25k$. *Finalmente sustituimos:*

$$x = 1 + 4k_1 = 1 + 4(15 + 25k) = 61 + 100k$$

b) *Puesto que* $27^{40} = 1$ *en* $\mathbb{Z}_{100}$ *tenemos que* $27^{36} \cdot 27^4 = 1$, *luego* $27^{36} = (27^4)^{-1}$.
Tenemos entonces que $27^4 = 729^2 = 29^2 = 841 = 41$. *Y ahora lo que hay es que calcular el inverso de* 41 *en* $\mathbb{Z}_{100}$.

r	c	v
100		*0*
41		*1*
18	*2*	*-2*
5	*2*	*5*
3	*3*	*-17*
2	*1*	*22*
1	*1*	*-39*

Luego $27^{36} = 41^{-1} = -39 = 61$.

c) *Vamos calculando las potencias.*

- $27^2 = 29$.
- $27^4 = 29^2 = 41$.
- $27^8 = 41^2 = 1681 = 81$.
- $27^{16} = 81^2 = 6561 = 61$.
- $27^{32} = 61^2 = 3721 = 21$.
- $27^{36} = 27^{32} \cdot 27^4 = 21 \cdot 41 = 861 = 61$.

De cualquiera de las formas que lo hagamos vemos que las dos últimas cifras son 61.

Nótese que empleando este método es indiferente que las congruencias estén expresadas de la forma $x \equiv b(\text{mód } m)$ o de la forma $ax \equiv b(\text{mód } m)$.
El siguiente algoritmo utiliza esta idea para resolver sistemas de congruencias.

Algoritmo SISTEMA$(p, (a_1, b_1, m_1), \cdots, (a_p, b_p, m_p))$

Entrada: $a, b \in \mathbb{Z}, m \in \mathbb{N} : m \geq 1$

$p \in \mathbb{N} : \ p \geq 2$
$a_1, \cdots, a_k, b_1, \cdots, b_k \in \mathbb{Z}$
$m_1, \cdots, m_k \in \mathbb{N}^*$

Salida: (c, n).

El sistema
$a_1 x \equiv b_1(\text{mód } m_1)$
$a_2 x \equiv b_2(\text{mód } m_2)$
$\cdots\cdots\cdots\cdots$
$a_p x \equiv b_p(\text{mód } m_p)$
y la congruencia $x \equiv c(\text{mód } n)$ son equivalentes.

$(c, n) :=$ CONGRUENCIA(a_1, b_1, m_1)
Desde $k = 2$ hasta p
$(a_k, b_k) := (a_k n, b_k - a_k c)$
$(u, v) :=$ CONGRUENCIA(a_k, b_k, m_k)
$(c, n) := (c + nu, nv)$
Devuelve (c, n)
Fin

Ejemplo 2.6.5. *Para terminar, vamos a calcular las dos últimas cifras del número* 125^{131} *expresado en hexadecimal (base 16).*

Llamemos x *a dicho número. Para calcular esas cifras, deberíamos calcular el cociente y el resto de dividir* x *entre 16 (llamemos a estos números* c_1 *y* r_1 *respectivamente. Y a continuación, calcular el resto de dividir* c_1 *entre 16. Si este número es* r_2*, las dos últimas cifras serán* r_2 *y* r_1 *(o sus correspondientes símbolos).*

El cálculo de r_1 *es fácil, pero no así el de* c_1*, lo que nos impediría calcular* r_2*.*

Supongamos que hemos logrado realizar esos cálculos. En ese caso, tendríamos:

$$x = 16 \cdot c_1 + r_1 = 16 \cdot (16 \cdot c_2 + r_2) + r_1 = 16^2 \cdot c_2 + (16 \cdot r_2 + r_1) = 256 \cdot c_2 + (16 \cdot r_2 + r_1)$$

Y vemos cómo $16 \cdot r_2 + r_1$ *es el resto de dividir* x *entre* 256*.*

Podemos entonces probar el siguiente camino:

- *Calculamos el resto de dividir* x *entre* $256 = 16^2$*. Llamemos* r *a dicho resto, y será un número comprendido entre 0 y 255.*
- *Dividimos* r *entre 16. El cociente y el resto serán las dos últimas cifras del número* x *en base 16.*

Procedemos a realizar los cálculos.

- *Hallamos el resto de dividir* x *entre 256. O lo que es lo mismo, reducimos* x *módulo 256.*

  Puesto que $mcd(125, 256) = 1$*, sabemos que* $125^{\varphi(256)} = 1$ *módulo 256. Y como* $256 = 2^8$*, entonces* $\varphi(256) = 2^8 - 2^7 = 128$*.*

  Por tanto, $125^{128} = 1$*, luego* $x = 125^{131} = 125^3 = 1953125 = 101$ *(en los cálculos se ha tenido en cuenta que trabajamos en* $\mathbb{Z}_{256}$*).*

- *Dividimos* 101 *entre 16. El resultado es* $101 = 6 \cdot 16 + 5$*.*

Las dos últimas cifras de x *en base 16 son entonces* 65*.*

Vamos a calcular el número x*.*

$x = 4956917651007127389207079210606530364889880565822452307824336564920852925565038035024233259874578684042313654409669718450394670590710208403868567104836288629763118163546279427505193009117663685236235990587462326272232025808101080123924814246905157233413774520158767700195312 5$

Y su expresión en base 16 es:

$16E84AD1CAC3DD6CEC6791668C39126FADD071D74AB8AA78DBC8F2C1F546253935407CB1DA9C62E4E0CBD48B6012ABCA409A571BEC47C5B8B18520495413745358E395EFE27A14C70DBB1EEB2DCC4ECE5AD3C7A37EDB78AEEFCBBC039C52521A26AAC5B6E21D71B22EE763322935769E0A702F65)$

Que como vemos termina en 65.

A partir de este ejemplo, podemos ver que un número x*, al escribirlo en hexadecimal, acaba en 65 si, y sólo si,* $x \equiv 101 (mód\ 16^2)$*.*

2.7. Ecuaciones diofánticas

Nos planteamos en esta sección resolver en $\mathbb{Z}$ ecuaciones de la forma

$$ax + by = c$$

donde $a, b, c \in \mathbb{Z}$. Fácilmente uno observa que estas ecuaciones no tienen siempre solución. Por ejemplo, la ecuación

$$8x + 20y = 135$$

no puede tener solución, pues para cualesquiera x e y números enteros, el miembro de la izquierda es un número par, luego no puede valer 135. Dicho de otra forma, el miembro de la derecha es múltiplo de 2, y el miembro de la izquierda no lo es.

Para tratar de generalizar este hecho, podemos verlo como que hemos encontrado un número d ($d = 2$) que verifica que $d|8$, $d|20$, pero $d \not| 135$.

Si pensamos ahora, por ejemplo en la ecuación $18x + 48y = 100$, ese razonamiento para $d = 2$ no nos sirve, pues todos los coeficientes que intervienen son múltiplos de 2. Vemos, no obstante que para $d = 3$ podemos razonar como en el ejemplo anterior (el miembro de la izquierda es múltiplo de 3 y no así el miembro de la derecha).

Repetir este razonamiento a una ecuación general de la forma $ax+by = c$ nos lleva a probar con todos los divisores comunes de a y b, pero dado que en el máximo común divisor de a y b están recogidos todos los divisores comunes de a y b, nos quedamos únicamente con éste.

Dada la ecuación $ax + by = c$, sea $d = mcd(a, b)$. Hemos razonado que una condición necesaria para que tenga solución es que d divida a c.

La siguiente proposición nos asegura que esta condición es también suficiente.

Proposición 2.7.1. *Sean $a, b, c \in \mathbb{Z}$ y $d = mcd(a, b)$. Entonces la ecuación*

$$ax + by = c$$

tiene solución entera si, y sólo si, $d|c$

Demostración: La condición necesaria ($ax + by = c$ tiene solución $\Longrightarrow$ $d|c$) es fácil de probar.

Veamos la condición suficiente (nos garantiza la existencia de solución).

Supongamos que $d|c$.

Planteamos la congruencia $\cong axcb$. Como $mcd(a, b)|c$ la congruencia tiene solución.

Sea $x = u$ una solución. Eso significa que $au - c$ es múltiplo de b, luego $au - c = bv$ para algún $v \in \mathbb{Z}$. Entonces $au - bv = c$, luego $x = u$, $y = -v$ es una solución de $ax + by = c$.

Además, si u', v' es otra solución de $ax+by = c$, entonces $au' - c$ es múltiplo de b, luego u' es solución de la congruencia $ax \equiv c(\text{mód } b)$. ■

La demostración anterior no sólo nos dice cuando una ecuación de la forma $ax+by = c$ tiene solución sino que nos proporciona una forma de encontrarlas.

Para ello, lo que tenemos es que resolver la congruencia $ax \equiv c(\text{mód } b)$ (o si preferimos, la congruencia $by \equiv c(\text{mód } a)$).

Ejemplo 2.7.1. *Vamos a encontrar, si es posible, una solución a la ecuación* $105x + 465y = 195$. *Para ello, planteamos la congruencia*

$$105x \equiv 195(mód\ 465)$$

Necesitamos calcular el máximo común divisor de 195 *y* 465. *Para ello, hacemos uso del algoritmo de Euclides.*

r	c
105	
465	
105	0
45	4
15	2
0	

Vemos que $mcd(105, 465) = 15$, *que divide a* 195 *(pues* $195 = 15 \cdot 13$*). La congruencia nos queda entonces* $7x \equiv 13(mód\ 31)$.

Calculamos el inverso de 7 *módulo* 31.

r	c	v
31		0
7		1
3	4	-4
1	2	9

Notemos que para calcular v podríamos haber aprovechado los cálculos que hicimos para el cálculo de $mcd(465, 105)$, pues la columna de los cocientes es la misma en ambos casos.

Vemos entonces que $7^{-1} = 9$. Multiplicando por 9 nos queda la congruencia $x \equiv 13 \cdot 9 (m\acute{o}d\ 31)$. Y como $13 \cdot 9 = 117$, que módulo 31 vale 24.

Luego $x = 24 + 31k$.

Sustituimos en la ecuación inicial:

$$105(24 + 31k) + 465y = 195$$

Y despejamos y:

$$y = \frac{195 - 105 \cdot 24 - 105 \cdot 31k}{465} = \frac{-2325 - 3255k}{465} = -5 - 7k$$

La solución de la ecuación $105x + 465y = 195$ es entonces:

$$\begin{array}{l} x = 24 + 31k \\ y = -5 - 7k \end{array} \qquad k \in \mathbb{Z}$$

Para cada valor de k obtenemos una solución distinta de la ecuación. Por ejemplo:

- *Para $k = 0$ tenemos $x = 24$, $y = -5$.*
- *Para $k = 1$ tenemos $x = 55$, $y = -12$.*
- *Para $k = -1$ tenemos $x = -7$, $y = 2$.*

Y todas esas parejas son soluciones de nuestra ecuación diofántica.

Proposición 2.7.2. *Sean $a, b, c \in \mathbb{Z}$ y $d = mcd(a, b)$. Supongamos que x_0, y_0 es una solución de la ecuación $ax + by = c$. Entonces todas las soluciones de esta ecuación son:*

$$\begin{array}{rcl} x & = & x_0 + k\,\frac{b}{d} \\ y & = & y_0 - k\,\frac{a}{d} \end{array} \qquad k \in \mathbb{Z}$$

Demostración: Se tiene que $a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right) = ax_0 + ak\frac{b}{d} + by_0 - bk\frac{a}{d} = ax_0 + by_0 + ak\frac{b}{d} - bk\frac{a}{d} = c$, luego todas las parejas (x, y) de la forma dada en el enunciado son soluciones.

Veamos que toda solución adopta esa forma. Sean $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$.

Si x, y es una solución de la ecuación, entonces $ax_0 + by_0 = ax + by$, de donde $a(x - x_0) + b(y - y_0) = 0$, es decir, $a(x - x_0) = b(y_0 - y)$, lo que implica que $a'(x - x_0) = b'(y_0 - y)$.

Se tiene entonces que $b' | a'(x - x_0)$, y como $mcd(a', b') = 1$ (¿por qué?) deducimos que $b' | (x - x_0)$, o sea, existe $k \in \mathbb{Z}$ tal que $x - x_0 = kb'$, de donde

$$x = x_0 + kb' = x_0 + k\frac{b}{d}$$

$b'(y_0 - y) = a'(x - x_0) = a'kb'$, luego $y_0 - y = ka'$, o, lo que es lo mismo, $y = y_0 - ka'$ ■

Ejemplo 2.7.2. *Notemos que en el ejemplo anterior tenemos que $x_0 = 24$, $y_0 = -5$ es una solución particular de la ecuación.*

Como $mcd(a, b) = 15$, la solución general adopta la forma

$$\begin{array}{l} x = 24 + \frac{465}{15}k \\ y = -5 - \frac{105}{15}k \end{array} \qquad k \in \mathbb{Z}$$

que es justamente la solución que nos ha salido.

La proposición 2.7.1 puede extenderse fácilmente al caso de ecuaciones diofánticas de 3 o más incógnitas. Por ejemplo, la ecuación $ax + by + cz = d$ tiene solución si, y sólo si, $mcd(a, b, c) | d$. Dar una expresión general de la solución, como hemos hecho en la proposición 2.7.2 no es tan sencillo.

Vamos a ver un ejemplo de cómo resolver una ecuación diofántica con tres incógnitas. El método puede ser fácilmente generalizado a 4 ó más.

Ejemplo 2.7.3. *Consideramos la ecuación* $6x + 10y + 15z = 23$. *Puesto que* $mcd(6, 10, 15) = 1$, *y 23 es múltiplo de 1, la ecuación tiene solución. Veamos cómo resolverla:*

- *Elegimos una incógnita (por ejemplo, z), y pasamos el término correspondiente al miembro de la derecha.*

$$6x + 10y = 23 - 15z$$

- *Consideramos entonces nuestra ecuación diofántica como una ecuación con dos incógnitas, y tratamos de resolverla.*
- *Puesto que* $mcd(6, 10) = 2$, *la ecuación tendrá solución si el término de la derecha es múltiplo de 2.*
- *Esta condición se traduce en una restricción sobre z. En nuestro caso es* $23 - 15z \equiv 0 (mód\ 2)$.
- *Resolvemos esta congruencia. La solución de esta congruencia es* $z = 1 + 2k$.
- *Sustituimos en la ecuación:* $6x + 10y = 23 - 15(1 + 2k)$, *lo que nos da* $6x + 10y = 8 - 46k$.
- *Transformamos esta ecuación en una congruencia:* $6x \equiv 8 - 46k (mód\ 10)$.
- *Estudiamos si tiene solución. Como* $mcd(6, 10) = 2$, *y* $8 - 46k$ *es múltiplo de 2, independientemente del valor de k, esta congruencia tiene solución para cualquier valor de k (de hecho, hemos elegido z para que esto ocurra).*
- *Resolvemos esta congruencia. Para ello, reducimos módulo 10 y dividimos todo por 2:* $3x \equiv 4 + 2k (mód\ 5)$.
- *Multiplicamos por 2, que es el inverso de 3 módulo 5:* $x \equiv 8 + 4k (mód\ 5)$, *o mejor,* $x \equiv 3 + 4k (mód\ 5)$.
- *Calculamos el valor de x:* $x = 3 + 4k + 5k'$.
- *Sustituimos:* $6(3 + 4k + 5k' + 10y = 8 - 46k$.
- *Despejamos y:*

$$y = \frac{8 - 46k - 6(3 + 4k + 5k')}{10} = \frac{8 - 46k - 18 - 24k - 30k'}{10} = \frac{-10 - 70k - 30k'}{10} = -1 - 7k - 3k'$$

Y ya tenemos resuelta la ecuación:

$$\begin{array}{rcrcrcrl} x & = & 3 & + & 4k & + & 5k' & \\ y & = & -1 & - & 7k & - & 3k' & \qquad k, k' \in \mathbb{Z} \\ z & = & 1 & + & 2k & & & \end{array}$$

Capítulo 3

Cuerpos finitos

En este capítulo vamos a construir cuerpos con un número finito de elementos. Esta construcción toma como base polinomios con coeficientes en $\mathbb{Z}_p$, con p un número primo. Antes de continuar, vamos a recordar qué es un cuerpo.

Sea A un conjunto no vacío. Decimos que A tiene estructura de anillo conmutativo si en A tenemos definidas dos operaciones:

$$\begin{array}{ccc} A \times A & \xrightarrow{+} & A \\ (a,b) & \mapsto & a+b \end{array} \qquad\qquad \begin{array}{ccc} A \times A & \xrightarrow{\cdot} & A \\ (a,b) & \mapsto & a \cdot b \end{array}$$

denominadas respectivamente suma y producto, y que satisfacen las siguientes propiedades:

i) Para cualesquiera $a, b, c \in A$ se tiene que $(a+b)+c = a+(b+c)$.

ii) Para cualesquiera $a, b \in A$ se tiene que $a+b = b+a$.

iii) Existe un elemento $0 \in A$ tal que $a+0 = a$ para cualquier $a \in A$.

iv) Para cualquier $a \in A$ existe un elemento $b \in A$ tal que $a+b = 0$.

v) Para cualesquiera $a, b, c \in A$ se tiene que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

vi) Para cualesquiera $a, b \in A$ se tiene que $a \cdot b = b \cdot a$.

vii) Existe un elemento $1 \in A$ tal que $a \cdot 1 = a$ para cualquier $a \in A$.

viii) Para cualesquiera $a, b, c \in A$ se tiene que $a \cdot (b+c) = a \cdot b + a \cdot c$.

Si además, se cumple la propiedad adicional:

ix) Para cualquier $a \in A$, $a \neq 0$ existe un elemento b tal que $a \cdot b = 1$

se dice que A tiene estructura de cuerpo.

Son ejemplos de anillos conmutativos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_n$, con $n \geq 2$. De todos estos, son cuerpos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$, con p un número primo.

Aunque en $\mathbb{N}$ también tenemos definidas una suma y un producto, $\mathbb{N}$ no es un anillo conmutativo, pues falla la propiedad iv).

La propiedad iv) nos habla de la existencia de un elemento $b \in A$ para cualquier $a \in A$ tal que $a+b = 0$. Hay un único elemento que cumple esa propiedad, y a ese elemento se le denomina *opuesto* de a, y se le suele denotar como $-a$.

De la misma forma, al elemento que nos define la propiedad ix) se le llama *inverso* de a, y se le denota como a^{-1}.

En un anillo conmutativo A, a los elementos que tienen inverso (es decir, elementos $a \in A$ para los que existe un elemento $b \in A$ tal que $a \cdot b = 1$) se les llama unidades.

Dados $a, b \in A$, escribiremos $a - b$ en lugar de $a + (-b)$.

A partir de la definición de anillo, se pueden deducir algunas propiedades, de todos conocidas:

1. $a \cdot 0 = 0$ sea quien sea $a \in A$.

2. (Regla de los signos) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ y $(-a) \cdot (-b) = a \cdot b$.
3. $-(a - b) = b - a$.

Coloquialmente hablando, podríamos decir que un anillo es un conjunto en el que podemos sumar, restar y multiplicar, con las propiedades usuales respecto a esas operaciones. Si además el producto es conmutativo, hablamos de un anillo conmutativo. Un cuerpo es un conjunto en el que podemos sumar, restar, multiplicar y dividir (salvo por cero).

3.1. Generalidades sobre polinomios

Definición 44. *Sea A un anillo conmutativo, y x un elemento que no pertenece a A. Un polinomio con coeficientes en A es una expresión de la forma*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

donde $n \in \mathbb{N}$ y $a_k \in A$.

Ejemplo 3.1.1. *Son polinomios con coeficientes en $\mathbb{Z}$*

$$2x^2 + 3x + (-1); \quad 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2$$

En el primer caso $n = 2$, $a_2 = 2$, $a_1 = 3$ y $a_0 = -1$, mientras que en el segundo $n = 5$ y $a_5 = a_4 = a_3 = a_2 = a_1 = a_0 = 2$.

No son polinomios con coeficientes en $\mathbb{Z}$

$$3x^2 - x + 2 + x^{-1}; \quad sen(x) - 3$$

Nota: La definición que se ha dado no es muy rigurosa. De hecho, con esa definición, la expresión $x^2 + 1$ no es un polinomio, pues no se ajusta a lo explicitado en dicha definición, ya que no está dicho quien es a_1 ni a_2. Sí es un polinomio, de acuerdo con la definición dada $1x^2 + 0x + 1$. Obviamente, al referirnos al polinomio $1x^2 + 0x + 1$ lo haremos como $x^2 + 1$. De la misma forma, el primer polinomio que aparece en el ejemplo anterior lo escribiremos $2x^2 + 3x - 1$.

En general, si $a_k x^k + \cdots + a_1 x + a_0$ es un polinomio y $a_i = 0$, entonces el polinomio dado diremos que es igual a $a_k x^k + \cdots + a_{i+1} x^{i+1} + a_{i-1} x^{i-1} + \cdots + a_0$ (salvo que el polinomio de partida sea 0).

Tampoco se ajusta a la definición que hemos dado de polinomio, por ejemplo, la expresión $5+2x+3x^2$. Deberíamos escribir $3x^2 + 2x + 5$.

En lo que sigue no tendremos en cuenta estas deficiencias de la definición dada.

Dado un anillo A denotaremos por $A[x]$ al conjunto de todos los polinomios con coeficientes en A.

Definición 45. *Sea A un anillo.*

1. *Sean $p(x) = a_m x^m + \cdots + a_1 x + a_0$ y $q(x) = b_n x^n + \cdots + b_1 x + b_0$ dos elementos de $A[x]$, y supongamos que $m \leq n$. Se define la suma de los polinomios $p(x)$ y $q(x)$ como el polinomio*

$$p(x) + q(x) = b_n x^n + \cdots + b_{m+1} x_{m+1} + (a_m + b_m) x^m + \cdots + (a_1 + b_1) x + (a_0 + b_0)$$

2. *Sea $k \in \mathbb{N}$, $p(x) = a_m x^m + \cdots + a_1 x + a_0$, $q(x) = b_k x^k \in A[x]$ (si $k = 0$ entonces $q(x) = b_0$). Se define el producto de $p(x)$ y $q(x)$ como el polinomio:*

$$p(x) \cdot q(x) = a_n b_k x^{k+n} + \cdots + a_1 b_k x^{k+1} + a_0 b_k x^k$$

Sean ahora $p(x) = a_m x^m + \cdots + a_1 x + a_0$ y $q(x) = b_n x^n + \cdots + b_1 x + b_0$. Se define el producto de $p(x)$ y $q(x)$ como

$$p(x) \cdot q(x) = p(x) \cdot q_n(x) + \cdots + p(x) \cdot q_1(x) + p(x) \cdot q_0(x)$$

donde $q_k(x) = b_k x^k$.

Las dos operaciones definidas satisfacen las siguientes propiedades:

- La suma de polinomios es asociativa, es decir, $p(x) + (q(x) + r(x)) = p(x) + q(x)) + r(x)$. Nótese que esta propiedad es necesaria para poder definir el producto tal y como se ha hecho aquí.
- La suma de polinomios es conmutativa.
- La suma tiene un elemento neutro. Éste será denotado por 0.
- Dado $p(x) \in A[x]$ existe $q(x) \in A[x]$ tal que $p(x) + q(x) = 0$. Denotaremos como $-p(x)$ a este polinomio.
- El producto de polinomios es asociativo y conmutativo.
- El producto tiene un elemento neutro. Éste será denotado por 1.
- La suma es distributiva con respecto al producto.

Estas propiedades nos dicen que, si A es un anillo conmutativo, entonces $A[x]$ es también un anillo conmutativo.

Además, podemos identificar A como los elementos de $A[x]$ de la forma $p(x) = a$, en cuyo caso A es un subanillo de $A[x]$.

Ejemplo 3.1.2. *Sea* $A = \mathbb{Z}_{12}$*, y sean* $p(x) = 2x^3 + 3x^2 + 7x + 9$ *y* $q(x) = 6x^2 + 5x + 4$*. Entonces:*

$* \; p(x) + q(x) = 2x^3 + (3+6)x^2 + (7+5)x + (9+4) = 2x^3 + 9x^2 + 1$

$$\begin{aligned} * \; p(x) \cdot q(x) &= p(x) \cdot (6x^2) + p(x) \cdot (5x) + p(x) \cdot 4 \\ &= (0x^5 + 6x^4 + 6x^3 + 6x^2) + (10x^4 + 3x^3 + 11x^2 + 9x) + (8x^3 + 0x^2 + 4x + 0) \\ &= 4x^4 + 5x^3 + 5x^2 + x \end{aligned}$$

Normalmente, para efectuar la multiplicación dispondremos los datos de la siguiente forma:

$p(x)$			2	3	7	9
$q(x)$				6	5	4
$p(x) \cdot 4$			8	0	4	0
$p(x) \cdot 5x$		10	3	11	9	
$p(x) \cdot 6x^2$	0	6	6	6		
$p(x) \cdot q(x)$	0	4	5	5	1	0

luego el resultado final es $4x^4 + 5x^3 + 5x^2 + x$*.*

Daremos a continuación algunos conceptos referentes a los polinomios:

Definición 46. *Sea* A *un anillo conmutativo y* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$*.*

i) Si $a_n \neq 0$ *entonces se dice que el polinomio* $p(x)$ *tiene* **grado** n *(*$gr(p(x)) = n$*). Nótese que no se ha definido el grado del polinomio* 0*. En ocasiones, consideraremos que el grado del polinomio* 0 *es* -1*.*

ii) Al elemento $a_k \in A$ *se le llama* **coeficiente de grado k***, y a la expresión* $a_k x^k$*,* **término de grado k***.*

iii) El coeficiente de grado n *de un polinomio de grado* n *se llama* **coeficiente líder***, y a la expresión* $a_n x^n$ **término líder***.*

iv) El coeficiente de grado 0 *de un polinomio se le llama* **término independiente***.*

v) Un polinomio cuyo coeficiente líder valga 1 *se dice que es un* **polinomio mónico***.*

vi) Un polinomio que, bien tiene grado 0*, o bien es el polinomio* 0 *se dice que es un* **polinomio constante***.*

Ejemplo 3.1.3. *Sean* $p(x) = 3x^3+5x+2$ *y* $q(x) = x^4+2x^3+3x^2+5x+8$ *dos polinomios con coeficientes en* $\mathbb{Z}_{11}$*. Entonces:*

- $gr(p(x)) = 3$ *y* $gr(q(x)) = 4$*.*

- El coeficiente de grado 2 *de* $p(x)$ *es* 0*, mientras que el coeficiente de grado* 2 *de* $q(x)$ *es* 3*. El coeficiente de grado* 5 *de* $q(x)$ *es cero.*

- El coeficiente líder de $p(x)$ *es* 3*, mientras que el coeficiente líder de* $q(x)$ *es* 1*. Por tanto,* $q(x)$ *es mónico, mientras que* $p(x)$ *no lo es.*

- Los términos independientes de $p(x)$ *y* $q(x)$ *son* 2 *y* 8 *respectivamente.*

- Ninguno de los dos polinomios son constantes.

Proposición 3.1.1. *Sean* $p(x), q(x) \in A[x]$*. Entonces:*

$$gr(p(x) + q(x)) \leq máx\{gr(p(x), q(x)\}$$

$$gr(p(x) \cdot q(x)) \leq gr(p(x)) + gr(q(x))$$

La demostración de ambos hechos es fácil. Podría pensarse que en el segundo caso se da siempre la igualdad ($gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$). Sin embargo, el Ejemplo 3.1.2 nos muestra un caso en el que se da la desigualdad estricta.

Es fácil comprobar que si $p(x)$ o $q(x)$ es mónico, entonces se verifica que $gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$.

Terminamos esta sección estudiando la evaluación de un polinomio en un punto.

Definición 47. *Sea* A *un anillo,* $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$ *y* $a \in A$*. Se define la evaluación de* $p(x)$ *en el punto* a*,* $Ev_a(p(x))$ *como el elemento de* A*:*

$$Ev_a(p(x)) = a_n a^n + \cdots + a_1 a + a_0$$

Dicho de otra forma, $Ev_a(p(x))$ es el resultado de sustituir en la expresión de $p(x)$ el símbolo x por a. De esta forma tenemos definida una aplicación (morfismo de anillos) $Ev_a : A[x] \to A$.

Normalmente, escribiremos $p(a)$ en lugar de $Ev_a(p(x))$.

Proposición 3.1.2. *Dado* A *un anillo y* $p_1(x), p_2(x) \in A[x]$

1. *Si* $q(x) = p_1(x) + p_2(x)$ *entonces* $q(a) = p_1(a) + p_2(a)$ *(es decir,* $Ev_a(p_1(x) + p_2(x)) = Ev_a(p_1(x)) + Ev_a(p_2(x))$*).*

2. *Si* $q(x) = p_1(x) \cdot p_2(x)$ *entonces* $q(a) = p_1(a) \cdot p_2(a)$ *(es decir,* $Ev_a(p_1(x) \cdot p_2(x)) = Ev_a(p_1(x)) \cdot Ev_a(p_2(x))$*).*

Usando la aplicación evaluación, cada polinomio de $A[x]$ determina una aplicación $A \to A$, dada por $a \mapsto p(a)$.

Ejemplo 3.1.4.

1. *El polinomio* $x^3 + 3x^2 + 2x + 2 \in \mathbb{Z}_5[x]$ *determina la aplicación* $\mathbb{Z}_5 \to \mathbb{Z}_5$ *siguiente:*

$$0 \mapsto 2 \quad 1 \mapsto 3 \quad 2 \mapsto 1 \quad 3 \mapsto 2 \quad 4 \mapsto 2$$

2. *El polinomio* $x^2 + x + 1 \in \mathbb{Z}_2[x]$ *determina la aplicación*

$$0 \mapsto 1 \qquad 1 \mapsto 1$$

es decir, la aplicación constante 1*.*

3.2. Máximo común divisor y mínimo común múltiplo

Definición 48. *Sean $p(x), q(x) \in A[x]$. Se dice que $p(x)$ divide a $q(x)$, o que $q(x)$ es múltiplo de $p(x)$, y escribiremos $p(x)|q(x)$, si existe $c(x) \in A[x]$ verificando que $q(x) = p(x) \cdot c(x)$.*

Ejemplo 3.2.1.

1. *En $\mathbb{Z}_2[x]$ se verifica que $(x+1)|(x^2+1)$, ya que $x^2+1 = (x+1)(x+1)$.*
2. *En $\mathbb{Z}_3[x]$ se verifica que $(x+1) \not| (x^2+1)$, pues si $x^2+1 = (x+1) \cdot c(x)$, entonces $gr(c(x)) = 1$, luego $c(x) = c_1x + c_0$. Operando resulta que $c_0 = 1$, $c_0 + c_1 = 0$ y $c_1 = 1$, lo cual es imposible.*
3. *En $\mathbb{Z}_4[x]$ se verifica que $(x+2)|(2x^2+x+2)$, pues $2x^2+x+2 = (x+2)(2x+1)$ y $(2x^2+x+2)|(x+2)$ pues $x+2 = (2x^2+x+2)(2x+1)$.*
4. *Para cualquier $p(x) \in A[x]$ se verifica que $1|p(x)$ y $p(x)|0$.*

En lo que sigue nos centraremos en polinomios con coeficientes en $\mathbb{Z}_p$, con p un número primo. Notemos que en todos los casos, el anillo de coeficientes es un cuerpo.

Veamos a continuación algunas propiedades referentes a la relación de divisibilidad de polinomios.

Proposición 3.2.1. *Sea K un cuerpo y $p(x), q(x), r(x) \in K[x]$. Entonces:*

1. *$1|p(x)$ y $p(x)|0$.*
2. *$p(x)|p(x)$.*
3. *Si $p(x)|q(x)$ y $q(x)|p(x)$, entonces existe $a \in K^*$ tal que $q(x) = a \cdot p(x)$.*
4. *Si $p(x)|q(x)$ y $q(x)|r(x)$, entonces $p(x)|r(x)$.*
5. *Si $p(x)|q(x)$ y $p(x)|r(x)$, entonces $p(x)|(q(x) + r(x))$.*
6. *Si $p(x)|q(x)$, entonces $p(x)|q(x) \cdot r(x)$ para cualquier $r(x) \in K[x]$.*

La demostración de estas propiedades es casi inmediata.

Teorema 3.2.1 (Algoritmo de la división)**.** *Sea K un cuerpo, y $p(x), q(x)$ dos polinomios de $K[x]$, con $q(x) \neq 0$. Entonces existen únicos polinomios $c(x), r(x) \in K[x]$ tales que:*

$p(x) = q(x) \cdot c(x) + r(x)$

$r(x) = 0$ *o* $gr(r(x)) < gr(q(x))$.

Los polinomios $c(x)$ y $r(x)$ son llamados cociente y resto respectivamente.

Demostración:
Vamos a dar una indicación de como sería la demostración de existencia.
Supongamos que $gr(q(x)) = m$ y que b_m es el coeficiente líder de $q(x)$.
Distingamos dos casos:

- $gr(p(x)) < m$. En tal caso, basta tomar $c(x) = 0$ y $r(x) = p(x)$.
- $gr(p(x)) \geq m$. Llamemos entonces n al grado de $p(x)$ y sea a_n su coeficiente líder. Sea entonces $c_1(x) = a_n \cdot (b_m)^{-1}x^{n-m}$ y $p_1(x) = p(x) - q(x) \cdot c_1(x)$. Se tiene entonces que:

- $p(x) = q(x) \cdot c_1(x) + p_1(x)$. Esto es evidente por cómo hemos definido $p_1(x)$.
- $gr(p_1(x)) < gr(p(x))$ o $p_1(x) = 0$. Esto es así porque el término líder de $q(x) \cdot c_1(x)$ vale $-a_n x^n$. Por tanto, al hacer la resta $p(x) - q(x) \cdot c_1(x)$, el coeficiente líder de $p(x)$ se anula con el coeficiente líder de $q(x) \cdot c_1(x)$.

Si ahora $gr(p_1(x)) < m$ (o $p_1(x) = 0$), ya hemos terminado. Basta tomar $c(x) = c_1(x)$ y $r(x) = p_1(x)$. En caso contrario, repetimos con $p_1(x)$ el mismo proceso que con $p(x)$.

Obtenemos así dos polinomios $p_2(x)$ y $c_2(x)$ tales que $p_1(x) = q(x) \cdot c_2(x) + p_2(x)$ y $gr(p_2(x)) < gr(p_1(x))$ o $p_2(x) = 0$. En tal caso, se tiene que:

$$p(x) = q(x) \cdot c_1(x) + p_1(x) = q(x) \cdot c_1(x) + q(x) \cdot c_2(x) + p_2(x) = q(x) \cdot (c_1(x) + c_2(x)) + p_2(x)$$

Obtenemos así dos sucesiones de polinomios $c_1(x), c_2(x), \cdots c_k(x)$ y $p_1(x), p_2(x), \cdots, p_k(x)$ satisfaciendo

- $p(x) = q(x) \cdot (c_1(x) + c_2(x) + \cdots + c_k(x)) + p_k(x)$
- $p_k(x) = 0$ ó $gr(p_k(x)) < gr(p_{k-1}(x)) < \cdots < gr(p_1(x)) < gr(p(x))$.

Este proceso lo continuamos hasta que $gr(p_k(x))$ sea menor que m o $p_k(x)$ sea igual al polinomio cero. En tal caso, basta tomar $c(x) = c_1(x) + \cdots + c_k(x)$ y $r(x) = p_k(x)$.

La demostración de la unicidad se deja como ejercicio.

■

Nótese que si en lugar de considerar un cuerpo consideramos un anillo conmutativo cualquiera, y $p(x), q(x)$ son dos polinomios tales que el coeficiente líder de $q(x)$ es una unidad, entonces podría repetirse la demostración.

Por tanto, si $p(x), q(x) \in A[x]$ y $q(x)$ es mónico, existe únicos $c(x), r(x) \in A[x]$ tales que $p(x) = q(x) \cdot c(x) + r(x)$, y $gr(r(x)) < gr(q(x))$ o $r(x) = 0$.

Ejemplo 3.2.2. *Calculemos el cociente y el resto de la división del polinomio* $p(x) = 2x^4 + 3x^3 + 5x + 1$ *entre* $q(x) = 3x^3 + x + 6$ *en* $\mathbb{Z}_7[x]$. *Lo haremos siguiendo los pasos hechos en la demostración precedente.*

Notemos en primer lugar que $gr(p(x)) > gr(q(x))$.

Calculamos 3^{-1}. *Se tiene que* $3^{-1} = 5$.

Tomamos entonces el polinomio $c_1(x) = 2 \cdot 5 \cdot x^{4-3} = 3x$.

Hallamos $p_1(x) = p(x) - 3xq(x) = p(x) + 4xq(x) = 3x^3 + 4x^2 + x + 1$.

Dado que $gr(p_1(x)) \geq gr(q(x))$ *continuamos dividiendo. Tomamos el polinomio* $c_2(x) = 3 \cdot 5x^{3-3} = 1$

Hallamos $p_2(x) = p_1(x) - 1q(x) = p_1(x) + 6q(x) = 4x^2 + 2$.

Dado que $gr(p_2(x)) < gr(q(x))$ *la división ha terminado. El cociente es* $c(x) = c_1(x) + c_2(x) = 3x + 1$ *y el resto* $r(x) = 4x^2 + 2$.

Los cálculos podemos disponerlos como sigue:

2	3	0	5	1	|	3	0	1	6
5	0	4	3			3	1		
	3	4	1	1					
	4	0	6	1					
		4	0	2					

Si analizamos el estudio que hicimos de los números enteros, podemos ver cómo el algoritmo de la división resultó clave en el desarrollo posterior. A partir de él se pudo probar la existencia de máximo común divisor y calcularlo; encontrar los coeficientes de Bezout, que luego fueron la base para la resolución de congruencias.

Ahora, en $\mathbb{Z}_p[x]$ tenemos también un algoritmo de división, luego todo lo dicho para números enteros vale también para polinomios.

En el capítulo anterior, a partir de un anillo (los números enteros), gracias al algoritmo de la división, construimos, para cada número primo p, un cuerpo que denominamos $\mathbb{Z}_p$.

Ahora, a partir de otro anillo ($\mathbb{Z}_p[x]$), y también apoyándonos en el algoritmo de la división, vamos a construir para cada polinomio irreducible $q(x)$ (que definiremos en su momento), un cuerpo que denominaremos $\mathbb{Z}_p[x]_{q(x)}$.

Nota: Un anillo A, se dice que es un dominio euclídeo si en él tenemos definida una aplicación *grado*, $g : A^* \to \mathbb{N}$ satisfaciendo dos propiedades:

- $g(ab) \geq g(a)$ para $b \neq 0$
- Para todo $a, b \in A$, $b \neq 0$, existen $q, r \in A$ tales que $a = bq + r$ y $g(r) < g(a)$ ó $r = 0$.

Es decir, un Dominio Euclídeo viene a ser un anillo en el que tenemos definida una división, con resto.

Tenemos entonces que $\mathbb{Z}$ y $K[x]$ son dominios euclídeos (las funciones grado son, en el caso de $\mathbb{Z}$ el valor absoluto, y en el caso de $K[x]$ el grado).

En un dominio euclídeo se verifica el teorema de Bezout, el teorema chino del resto, el teorema de factorización única, etc.

Definición 49. *Sean $p(x), q(x) \in K[x]$, con $q(x) \neq 0$. Se definen los polinomios $p(x)$ mód $q(x)$ y $p(x)$ div $q(x)$ como el resto y el cociente de dividir $p(x)$ entre $q(x)$.*

Cuando $p(x)$ mód $q(x) = 0$, denotaremos por $\frac{p(x)}{q(x)}$ al polinomio $p(x)$ div $q(x)$.

Ejemplo 3.2.3.

1. *En $\mathbb{Z}_3[x]$, se verifica que:*

   $$x^5 + x^4 + 2x^3 + x^2 + x + 1 \text{ mód } x^2 + 2x + 1 = 2$$
   $$x^5 + x^4 + 2x^3 + x^2 + x + 1 \text{ div } x^2 + 2x + 1 = x^3 + 2x^2 + 2.$$

2. *En $\mathbb{Z}_5[x]$:*

   $$x^5 + x^4 + 2x^3 + x^2 + x + 1 \text{ mód } x^2 + 2x + 1 = 6x$$
   $$x^5 + x^4 + 2x^3 + x^2 + x + 1 \text{ div } x^2 + 2x + 1 = x^3 + 4x^2 + 3x + 1.$$

Definición 50. *Sea $p(x) \in K[x]$ y $a \in K$. Se dice que a es una raíz de $p(x)$ si $p(a) = 0$.*

Ejemplo 3.2.4. *El polinomio $p(x) = x^5 + x^4 + x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$ tiene a $x = 1$ por raíz, pues $p(1) = 1 + 1 + 1 + 2 + 1 = 0$. Sin embargo, 0 no es raíz pues $p(0) = 1$ y 2 tampoco es raíz pues $p(2) = 2^5 + 2^4 + 2^3 + 2 \cdot 2^2 + 1 = 2 + 1 + 2 + 2 + 1 = 2$.*

El siguiente resultado es un conocido teorema referente a la división por el polinomio $x - a$.

Teorema 3.2.2 (Teorema del resto)**.** *Sea $p(x) \in K[x]$ y $a \in K$. Entonces el resto de dividir $p(x)$ entre $x - a$ es el resultado de evaluar $p(x)$ en el punto a. Dicho de otra forma*

$$p(x) \text{ mód } x - a = p(a)$$

Demostración: Si dividimos $p(x)$ entre $x-a$ nos da un polinomio de grado menor que 1, luego debe ser un polinomio constante. Se tiene entonces que $p(x) = c(x)\cdot(x-a)+r$. Evaluando en a nos queda que $p(a) = c(a)\cdot(a-a)+r$, es decir, $r = p(a)$. ■

Corolario 3.2.1 (Teorema del factor). *Sea $p(x) \in K[x]$ y $a \in K$. Entonces a es raíz de $p(x)$ si, y sólo si, $(x-a)|p(x)$.*

Nota: Si trabajamos con polinomios con coeficientes en un anillo conmutativo cualquiera (por ejemplo, $\mathbb{Z}$, o $\mathbb{Z}_n$ con n un número compuesto), los resultados anteriores son igualmente válidos.

En la siguiente proposición veremos una forma rápida de calcular el cociente y el resto de la división de un polinomio entre $x-a$.

Proposición 3.2.2. *Sea $p(x) \in K[x]$, $a \in K$. Supongamos que $p(x) = a_n x^n + \cdots + a_1 x + a_0$ y que $p(x) = (b_{n-1}x^{n-1} + \cdots + b_1 x + b_0)(x-a) + r$. Entonces:*

$b_{n-1} = a_n$

$b_{i-1} = a_i + b_i a$ *para* $i = 0, 1, \cdots, n-1$

$r = a_0 + b_0 a$

La demostración se deja como ejercicio.

Esta proposición proporciona el conocido método de Ruffini (algoritmo de Horner) para dividir un polinomio entre $x-a$.

Para esto se disponen los datos conocidos como sigue:

	a_n	a_{n-1}	$\cdots$	a_{i+1}	a_i	$\cdots$	a_1	a_0
a								
	b_{n-1}	b_{n-2}	$\cdots$	b_i	b_{i-1}	$\cdots$	b_0	r

Para calcular los coeficientes b_i se procede como sigue:

Se comienza por $b_{n-1} = a_n$

Supuesto calculado b_i se calcula b_{i-1} como $b_{i-1} = a_i + b_i a$.

Por último, hallado b_0 se calcula r como $r = a_0 + b_0 a$.

Para ordenar los cálculos se coloca el valor $b_i a$ justo debajo del valor de a_i, y se efectúa la suma, obteniéndose así el valor de b_{i-1}.

	a_n	a_{n-1}	$\cdots$	a_{i+1}	a_i	$\cdots$	a_1	a_0
a					$b_i a$			
	$b_{n-1} = a_n$	b_{n-2}	$\cdots$	b_i	$b_{i-1} = a_i + b_i a$	$\cdots$	b_0	r

Ejemplo 3.2.5. *Vamos a hallar el cociente y el resto de la división de $x^5 + x^4 + x^3 + 2x^2 + 1$ entre $x + 9 = x - 2$ en $\mathbb{Z}_{11}[x]$. Para ello procedemos a completar la tabla*

	1	1	1	2	0	1
2						

Rellenando de izquierda a derecha.

	1	1	1	2	0	1
2		$2 = 1\cdot 2$	$6 = 3\cdot 2$	$3 = 7\cdot 2$	$10 = 5\cdot 2$	$9 = 10\cdot 2$
	1	$3 = 1+2$	$7 = 1+6$	$5 = 2+3$	$10 = 0+10$	$10 = 1+9$

La tabla quedaría así

	1	1	1	2	0	1
2		2	6	3	10	9
	1	3	7	5	10	10

Nótese que $x^5+x^4+x^3+2x^2+1=(x^4+3x^3+7x^2+5x+10)(x+9)+10$, *y que* $p(2)=10$.

Vamos a dividir ahora $x^5+x^4+x^3+2x^2+1$ *entre* $x+1$ *en* $\mathbb{Z}_3[x]$. *Puesto que* $x+1=x-2$, *se tiene que*

	1	1	1	2	0	1
2		2	0	2	2	1
	1	0	1	1	2	2

es decir, el cociente es x^4+x^2+x+2 *y el resto es* 2.

Definición 51. *Sea* $p(x)\in K[x]$, *y* $a\in K$. *Se dice que* a *es una raíz de multiplicidad* m *si* $(x-a)^m|p(x)$ *y* $(x-a)^{m+1}\not|p(x)$.

Nótese que decir que a es una raíz de multiplicidad m es decir que $p(x)=(x-a)^m c(x)$ con $c(a)\neq 0$.

A las raíces de multiplicidad 1 se les llama raíces simples; a las de multiplicidad 2, raíces dobles, a las de multiplicidad 3, raíces triples, y así sucesivamente.

En ocasiones, si a no es una raíz se dice que es una raíz de multiplicidad 0.

Ejemplo 3.2.6. *El polinomio* $x^5+x^3+x^2+1\in\mathbb{Z}_2[x]$ *tiene a* $x=1$ *como raíz triple, pues* $x^5+x^3+x^2+1=(x+1)^3(x^2+x+1)$, *y* x^2+x+1 *no tiene a* 1 *como raíz.*

	1	0	1	1	0	1
1		1	1	0	1	1
	1	1	0	1	1	0
1		1	0	0	1	
	1	0	0	1	0	
1		1	1	1		
	1	1	1	0		
1		1	0			
	1	0	1			

Aquí vemos las sucesivas divisiones por $x+1$. *Se aprecia como las tres primeras son exactas, mientras que la cuarta da resto* 1.

Definición 52. *Sea* K *un cuerpo, y* $p(x),q(x)\in K[x]$. *Se dice que* $d(x)\in K[x]$ *es un máximo común divisor de* $p(x)$ *y* $q(x)$ *si:*

1. $d(x)|p(x)$ *y* $d(x)|q(x)$.
2. *Si* $c(x)|p(x)$ *y* $c(x)|q(x)$ *entonces* $c(x)|d(x)$.

Nota:

1. La primera condición de la definición nos dice que $d(x)$ debe ser un divisor común de $p(x)$ y $q(x)$. La segunda condición nos dice que este divisor común es el "más grande" de los divisores comunes.

   El máximo común divisor de dos polinomios $p(x)$ y $q(x)$ es entonces un polinomio que es divisor común de ambos polinomios, y que es múltiplo de todos los divisores comunes.

2. Si $d(x)$ es un máximo común divisor de $p(x)$ y $q(x)$ y $a \in K^*$ entonces $a \cdot d(x)$ es también un máximo común divisor de $p(x)$ y $q(x)$. De hecho, cualquier polinomio que sea un máximo común divisor de $p(x)$ y $q(x)$ es de la forma $a \cdot d(x)$. De todos estos, hay uno, y sólo uno que es mónico (salvo en el caso de que $p(x) = q(x) = 0$). Denotaremos por $mcd(p(x), q(x))$ al único máximo común divisor de $p(x)$ y $q(x)$ que es mónico.

3. Aquí se ha definido el máximo común divisor de dos polinomios. Podría haberse definido de forma análoga el máximo común divisor de 3 ó más.

Ejemplo 3.2.7. *Sean $p(x) = x^2 + 4x + 4$ y $q(x) = x^2 + 1$. El polinomio $p(x)$ tiene 12 divisores. Estos son:*

$$1, 2, 3, 4, x+2, 2x+4, 3x+1, 4x+3, x^2+4x+4, 2x^2+3x+3, 3x^2+2x+2, 4x^2+x+1$$

mietras que $q(x)$ tiene 16, que son:

$$1, 2, 3, 4, x+2, 2x+4, 3x+1, 4x+3, x+3, 2x+1, 3x+4, 4x+2, x^2+1, 2x^2+2, 3x^2+3, 4x^2+4$$

El conjunto de los divisores comunes de $p(x)$ y $q(x)$ es:

$$\{1,\ 2,\ 3,\ 4,\ x+2,\ 2x+4,\ 3x+1,\ 4x+3\}$$

De ellos:

- *$x + 2$ es múltiplo de todos, pues $x + 2 = 1 \cdot (x + 2)$, $x + 2 = 2 \cdot (3x + 1)$, $x + 2 = 3 \cdot (2x + 4)$, $x + 2 = 4 \cdot (4x + 3)$. Por tanto, $x + 2$ es un máximo común divisor de $p(x)$ y $q(x)$.*
- *$2x + 4$ es múltiplo de todos, pues $2x + 4 = 1 \cdot (2x + 4)$, $2x + 4 = 2 \cdot (x + 2)$, $2x + 4 = 3 \cdot (4x + 3)$, $2x + 4 = 4 \cdot (3x + 1)$, luego $2x + 4$ es también un máximo común divisor de $p(x)$ y $q(x)$.*
- *$3x + 1$ es múltiplo de todos, ya que $3x + 1 = 1 \cdot (3x + 1)$, $3x + 1 = 2 \cdot (4x + 3)$, $3x + 1 = 3 \cdot (x + 2)$, $3x + 1 = 4 \cdot (2x + 4)$. También $xx + 1$ es un máximo común divisor de $p(x)$ y $q(x)$.*
- *$4x + 3$ es múltiplo de todos: $4x + 3 = 1 \cdot (4x + 3)$, $4x + 3 = 2 \cdot (2x + 4)$, $4x + 3 = 3 \cdot (3x + 1)$, $4x + 3 = 4 \cdot (x + 2)$. Es decir, $4x + 3$ es un máximo común divisor de $p(x)$ y $q(x)$.*

Vemos entonces que $p(x)$ tiene cuatro polinomios que satisfacen la definición de máximo común divisor. Son $x + 2$, $2x + 4$, $3x + 1$ y $4x + 3$. Elegido uno cualquiera de ellos, $d(x)$, podemos ver que los restantes son $2 \cdot d(x)$, $3 \cdot d(x)$ y $4 \cdot d(x)$.
Vemos también que hay uno que es mónico, y es $x+2$. Escribiremos por tanto $mcd(p(x), q(x)) = x+2$.

Se deja como ejercicio dar la definición de mínimo común múltiplo.
Veremos a continuación algunas propiedades referentes al máximo común divisor. Supongamos que tenemos $p(x), q(x), r(x), d(x) \in K[x]$, y supondremos que los cuatro polinomios son mónicos.

Propiedades:

1. $mcd(p(x), q(x)) = mcd(a \cdot p(x), q(x)) = mcd(p(x), a \cdot q(x))$, donde $a \in K^*$.
2. $mcd(p(x), 0) = p(x)$ y $mcd(p(x), 1) = 1$
3. Si $p(x)|q(x)$ entonces $mcd(p(x), q(x)) = p(x)$.
4. $mcd(p(x), mcd(q(x), r(x)) = mcd(mcd(p(x), q(x)), r(x)) = mcd(p(x), q(x), r(x))$.
5. $mcd(p(x) \cdot r(x), q(x) \cdot r(x)) = mcd(p(x), q(x)) \cdot r(x)$
6. Si $d(x)|p(x)$ y $d(x)|q(x)$ entonces $mcd\left(\frac{p(x)}{d(x)}, \frac{q(x)}{d(x)}\right) = \frac{mcd(p(x),q(x))}{d(x)}$.

Los siguientes resultados son análogos a los dados para números enteros.

Lema 3.2.1. *Sean $p(x), q(x) \in K[x]$. Entonces, para cualquier $c(x) \in K[x]$ se tiene que $mcd(p(x), q(x)) = mcd(q(x), p(x) - c(x)q(x))$.*

Corolario 3.2.2. *Sean $p(x), q(x) \in K[x]$, con $q(x) \neq 0$. Entonces $mcd(p(x), q(x)) = mcd(q(x), p(x) \text{ mód } q(x))$.*

Para calcular ahora el máximo común divisor de dos polinomios procedemos de igual forma que a la hora de calcular el máximo común divisor de dos números enteros. Vamos realizando divisiones hasta obtener un resto nulo. El resto anterior es el máximo común divisor.

$$\begin{array}{rcl} p(x) & = & q(x) \cdot c_1(x) \ + \ r_1(x) \\ q(x) & = & r_1(x) \cdot c_2(x) \ + \ r_2(x) \\ r_1(x) & = & r_2(x) \cdot c_3(x) \ + \ r_3(x) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ r_{i-2}(x) & = & r_{i-1}(x) \cdot c_i(x) \ + \ r_i(x) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ r_{k-2}(x) & = & r_{k-1}(x) \cdot c_k(x) \ + \ r_k(x) \\ r_{k-1}(x) & = & r_k(x) \cdot c_{k+1}(x) + 0 \end{array}$$

Sin embargo, el polinomio $r_k(x)$ no tiene por qué ser mónico, luego el resultado final, $r_k(x)$, no sería el máximo común divisor de $p(x)$ y $q(x)$. Necesitamos multiplicar por el inverso del coeficiente líder para obtener el máximo común divisor.

El algoritmo EUCLIDES del capítulo anterior vale ahora para el cálculo del máximo común divisor de dos polinomios con coeficientes en un cuerpo. Únicamente, al final hay que multiplicar el resultado por el inverso del coeficiente líder de $p(x)$.

En el caso de que los dos polinomios, $p(x)$ y $q(x)$ fueran nulos, el algoritmo daría error.

Algoritmo EUCLIDES$(p(x), q(x))$

Entrada: $p(x), q(x) \in K[x]$

Salida: $d(x) = mcd(p(x), q(x))$

  Mientras $q(x) \neq 0$

    $(p(x), q(x)) := (q(x), p(x) \text{ mód } q(x))$

$a = c.l.(p(x))^{-1}$.

$p(x) := a \cdot p(x)$.

Devuelve $p(x)$

Ejemplo 3.2.8.

1. *Vamos a calcular el máximo común divisor de los polinomios $p(x)$ y $q(x)$ del ejemplo 3.2.7. Para esto, vamos realizando las divisiones sucesivas hasta que nos dé resto cero.*

   - $x^2 + 4x + 4 = (x^2 + 1) \cdot 1 \ + \ 4x + 3$.
   - $x^2 + 1 = (4x + 3) \cdot (4x + 2) \ + 0$.

   Y al haber obtenido resto cero, tenemos que un máximo común divisor es $4x + 3$ (último resto no nulo). Multiplicamos por el inverso del coeficiente líder (es decir, multiplicamos por 4), y tenemos que $mcd(p(x), q(x)) = 4 \cdot (4x + 3) = x + 2$.

2. *Vamos a calcular en* $\mathbb{Z}_5[x]$ *el máximo común divisor de* x^3+4x+3 *y* x^3+x^2+1.

$$\begin{array}{rcrcrr} x^3+4x+3 & = & (x^3+x^2+1) & 1 & + & (4x^2+4x+2) \\ x^3+x^2+1 & = & (4x^2+4x+2) & (4x) & + & 2x+1 \\ 4x^2+4x+2 & = & (2x+1) & (2x+1) & + & 1 \end{array}$$

Luego el máximo común divisor de x^3-x+3 *y* x^3+x^2+1 *es* 1.

El teorema de Bezout se tiene también en el caso de los polinomios.

Teorema 3.2.3. *Sean* $p(x), q(x) \in K[x]$, *y sea* $d(x) = mcd(p(x), q(x))$. *Entonces existen* $u(x), v(x) \in K[x]$ *tales que* $d(x) = p(x)\cdot u(x) + q(x)\cdot v(x)$

La demostración del teorema, así como el algoritmo para calcular $u(x)$ y $v(x)$ es análogo al hecho en el caso de los números enteros. Hay que tener en cuenta que al final, hay que multiplicar el resultado por el inverso del coeficiente líder.

Algoritmo BEZOUT$(p(x), q(x))$
Entrada: $p(x), q(x) \in K[x]$
Salida: $(d(x), u(x), v(x))$: $d(x) = mcd(p(x), q(x))$; $d(x) = p(x)\cdot u(x) + q(x)\cdot v(x)$
  Si $q(x) = 0$
    $a := c.l.(p(x))^{-1}$
    Devuelve $(a\cdot p(x), a, 0)$;
    Fin
  $r_{-1}(x) := p(x)$, $r_0(x) := q(x)$.
  $u_{-1}(x) := 1$, $u_0(x) := 0$.
  $v_{-1}(x) := 0$, $v_0(x) := 1$.
  $i := 1$.
  $r_1(x) := r_{-1}(x)$ mód $r_0(x)$
  Mientras $r_i(x) \neq 0$
    $c_i(x) := r_{i-2}(x)$ div $r_{i-1}(x)$.
    $u_i(x) := u_{i-2}(x) - u_{i-1}(x)\cdot c_i(x)$.
    $v_i(x) := v_{i-2}(x) - v_{i-1}(x)\cdot c_i(x)$.
    $i := i+1$.
    $r_i(x) := r_{i-2}(x)$ mód $r_{i-1}(x)$.
  $a := c.l.(r_{i-1}(x))^{-1}$
  $r(x) := a\cdot r_{i-1}(x)$; $u(x) := a\cdot u_{i-1}(x)$; $v(x) := a\cdot v_{i-1}(x)$.
  Devuelve $(r(x), u(x), v(x))$.
  Fin

Ejemplo 3.2.9.

1. *Vamos a expresar* $mcd(x^3+4x+3, x^3+x^2+1)$ *en función de los polinomios* x^3-x+3 *y* x^3+x^2+1.

i	a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
-1		x^3+4x+3		1	0
0		x^3+x^2+1		0	1
1		$4x^2+4x+2$	1	1	4
2		$2x+1$	$4x$	x	$4x+1$
3		1	$2x+1$	$\mathbf{3x^2+4x+1}$	$\mathbf{2x^2+4x+3}$

Aquí vemos cómo se han obtenido las dos últimas columnas:

$1 = 1 - 1 \cdot 0$
$x = 0 - (4x) \cdot 1$
$3x^2 + 4x + 1 = 1 - (2x+1) \cdot x = 1 + (3x+4) \cdot x$

$4 = 0 - 1 \cdot 1$
$4x + 1 = 1 - (4x) \cdot (4)$
$2x^2 + 4x + 3 = 4 - (2x+1) \cdot (4x+1) = 4 + (3x+4) \cdot (4x+1)$

Nótese que se verifica que

$$1 = (x^3 + 4x + 3)(3x^2 + 4x + 1) + (x^3 + x^2 + 1)(2x^2 + 4x + 3)$$

2. *Sean* $p(x) = x^5 + 2x^4 + x^2 + 2x + 2$, $q(x) = x^5 + 2x^3 + x^2 + x + 1 \in \mathbb{Z}_3[x]$. *Vamos a calcular su máximo común divisor y a exprearlo en función de* $p(x)$ *y* $q(x)$.

i	a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
-1		$x^5 + 2x^4 + x^2 + 2x + 2$		1	0
0		$x^5 + 2x^3 + x^2 + x + 1$		0	1
1		$2x^4 + x^3 + x + 1$	1	1	2
2		$2x^2 + 2$	$2x + 2$	$x + 1$	$2x$
3	2	0			
		$\mathbf{x^2 + 1}$		$\mathbf{2x + 2}$	$\mathbf{x}$

Luego $mcd(x^5 + 2x^4 + x^2 + 2x + 2, x^5 + 2x^3 + x^2 + x + 1) = x^2 + 1$ *y*

$$x^2 + 1 = (x^5 + 2x^4 + x^2 + 2x + 2)(2x + 2) + (x^5 + 2x^3 + x^2 + x + 1)(x)$$

En el primer ejemplo, como el último resto distinto de cero es mónico, no ha sido necesario multiplicar por el inverso del coeficiente líder. En el segundo ejemplo, el último resto no nulo era $2x^2 + 2$, *que no es mónico. Por tanto, hemos tenido que multiplicar tanto* $u(x)$ *como* $v(x)$ *por el inverso del coeficiente líder.*

Los Corolarios 2.3.2, 2.3.3 y 2.3.4, así como la Proposición 2.3.1 pueden ahora trasladarse al contexto de polinomios con coeficientes en un cuerpo.

3.3. Factorización de polinomios en $\mathbb{Z}_p[x]$

Para la construcción de los cuerpos finitos, necesitamos el concepto análogo al de número primo en el contexto de polinomios con coeficientes en $\mathbb{Z}_p$.

Comenzamos con la definición de polinomios irreducibles.

Definición 53. *Sea* $p(x) \in K[x]$ *no constante. Se dice que* $p(x)$ *es irreducible si sus únicos divisores son los polinomios constantes (no nulos) y los polinomios de la forma* $a \cdot p(x) : a \in K^*$.
Si $p(x)$ *no es irreducible, se dice que es reducible.*

Observación: Nótese que si $p(x) \in K[x]$ es reducible y $gr(p(x)) = n$ entonces $p(x)$ tiene un divisor no constante, mónico, de grado menor o igual que $\frac{n}{2}$.

Ejemplo 3.3.1.

1. *Cualquier polinomio de grado* 1 *en* $K[x]$ *es irreducible.*

2. *El polinomio* $x^3+x+1 \in \mathbb{Z}_2[x]$ *es irreducible. Si fuera reducible, por la observación anterior debería tener un divisor de grado menor o igual que* $\frac{3}{2}$*. Los únicos polinomios en esas condiciones son* x *y* $x+1$*, y ninguno de ellos divide a* x^3+x+1*.*

3. *Dado* $p(x) = ax^2+bx+c \in \mathbb{R}[x]$ *entonces* $p(x)$ *es irreducible si, y sólo si,* $b^2-4ac<0$*.*

Al igual que teníamos en $\mathbb{Z}$, tenemos ahora una caracterización de los polinomios irreducibles.

Proposición 3.3.1. *Sea* $p(x) \in K[x]$ *no constante. Entonces:*

$$p(x) \text{ es irreducible} \iff \big(p(x)|q_1(x)\cdot q_2(x) \Longrightarrow p(x)|q_1(x) \text{ ó } p(x)|q_2(x)\big)$$

Con esta proposición estamos ya en condiciones de dar el teorema de factorización.

Teorema 3.3.1. *Sea* K *un cuerpo, y* $p(x) \in K[x]$ *no constante. Entonces* $p(x)$ *se expresa de forma única como*

$$p(x) = ap_1(x)p_2(x)\cdots p_k(x)$$

donde $a \in K$ *y* $p_i(x)$ *es un polinomio mónico e irreducible.*

La demostración es similar a la que se hizo del teorema fundamental de la aritmética.

En $\mathbb{Z}_8[x]$ se tiene que $x^2+7 = (x+1)(x+7) = (x+3)(x+5)$. Vemos entonces que podemos factorizar un polinomio de dos formas distintas. Sin embargo, puesto que $\mathbb{Z}_8$ no es un cuerpo, este ejemplo no está en contradicción con la afirmación de la factorización única que nos da el teorema 3.3.1.

Dado un polinomio $q(x) \in \mathbb{Z}_p[x]$ que no sea una potencia de un polinomio irreducible, existe un algoritmo (algoritmo de Berlekamp) que nos proporciona un divisor propio de este polinomio, caso de existir. Sin embargo, ese algoritmo escapa de los objetivos de estas notas, por lo que no lo estudiaremos aquí. Para factorizar un polinomio, seguiremos el método de ensayo-error.

Si tenemos un número entero, y queremos descomponerlo como producto de números primos, la forma más sencilla para hacerlo (aunque no la más eficiente, especialmente si se trata de números grandes) es ir probando con cada uno de los números primos, para ver si hay alguno que lo divida. Normalmente, comenzamos probando con el primo $p=2$, si no lo divide seguimos con el primo $p=3$ y así sucesivamente. En prncipio, habría que seguir hasta que encontremos un divisor primo, o hasta que hayamos llegado a la raíz cuadrada del número a factorizar.

Ahora, si tenemos un polinomio $q(x) \in \mathbb{Z}_p[x]$ de grado n, seguiremos una estrategia análoga. Probaremos por los irreducibles de grado uno, si ninguno lo divide pasaremos a los irreducibles de grado 2, y así sucesivamente, bien hasta que encontremos un divisor irreducible, bien hasta que hayamos probado por todos los irreducibles de grado menor o igual que $\frac{n}{2}$.

Supongamos que tenemos un polinomio $q(x) \in \mathbb{Z}_p[x]$ que queremos factorizar. Como acabamos de comentar, lo primero que hemos de hacer es comprobar si lo divide algún polinomio mónico de grado 1. Los polinomios mónicos de grado 1 son $x, x+1, \cdots, x+(p-1)$. Por tanto, tenemos que comprobar si el resto de la división de $q(x)$ por alguno de estos polinomios vale o no cero. Pero los restos de estas divisiones son respectivamente $q(0),\ q(p-1), \cdots, q(1)$ (ver teorema 3.2.2).

Entonces, lo primero que hemos de hacer para factorizar un polinomio $q(x) \in \mathbb{Z}_p[x]$ es ver si tiene raíces o no.

Ejemplo 3.3.2.

1. *Sea* $p(x) = x^3+x+1 \in \mathbb{Z}_2[x]$*. Entonces* $p(0)=1$ *y* $p(1)=1$*. Como* $\mathbb{Z}_2 = \{0,1\}$*, el polinomio* $p(x)$ *no tiene raíces.*

   Con esto, sabemos que el polinomio no tiene divisores de grado 1. Dado que $p(x)$ *tiene grado 3 esto es suficiente para asegurarnos que el polinomio es irreducible.*

2. *Sea ahora* $p(x) = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$. *Al igual que antes, podemos comprobar que este polinomio no tiene raíces (pues* $p(0) = p(1) = 1$*). Sin embargo, esto no es suficiente para asegurar que el polinomio sea irreducible (de hecho, este polinomio es reducible, pues* $x^4 + x^2 + 1 = (x^2 + x + 1)^2$*).*

3. *Sea ahora* $p(x) = x^3 + x + 1 \in \mathbb{Z}_3[x]$. *Ahora se tiene que* $p(1) = 0$*, luego* $x = 1$ *es una raíz. Probamos a dividir por* $x - 1$.

	1	0	1	1
1		1	1	2
	1	1	2	0

Luego $p(x) = (x + 2) \cdot (x^2 + x + 2)$. *Puede comprobarse fácilmente que* $x^2 + x + 2$ *no tiene raíces, y por ser de grado 2 tendríamos que es irreducible.*

4. *Sea* $p(x) = x^4 + 3x^3 + 2x^2 + 6x + 5 \in \mathbb{Z}_7[x]$. *Vamos a encontrar sus raíces. Para eso, vamos a ir probando por los distintos elementos de* $\mathbb{Z}_7$. *Claramente,* $p(0) = 5 \neq 0$.

	1	3	2	6	5
1		1	4	6	5
	1	4	6	5	3

	1	3	2	6	5
2		2	3	3	4
	1	5	5	2	2

	1	3	2	6	5
3		3	4	4	2
	1	6	6	3	0

Luego $x = 3$ *es una raíz, y* $p(x) = (x - 3) \cdot (x^3 + 6x^2 + 6x + 3)$. *Ahora seguimos buscando raíces, pero lo hacemos con el polinomio* $x^3 + 6x^2 + 6x + 3$. *Con* $x = 0$, $x = 1$ *y* $x = 2$ *ya no tenemos que probar, pues lo hemos hecho antes.*

	1	6	6	3
3		3	6	1
	1	2	5	4

	1	6	6	3
4		4	5	2
	1	3	4	5

	1	6	6	3
5		5	6	4
	1	4	5	0

Y vemos que $x = 5$ *es otra raíz. Tenemos entonces que* $p(x) = (x - 3) \cdot (x - 5) \cdot (x^2 + 4x + 5)$. *Continuamos ahora con* $x^2 + 4x + 5$.

	1	4	5
5		5	3
	1	2	1

	1	4	5
6		6	4
	1	3	2

Y por tanto, $p(x)$ *no tiene más raíces. Tendríamos entonces la siguiente factorización del polinomio* $p(x)$*:*

$$p(x) = (x + 4) \cdot (x + 2) \cdot (x^2 + 4x + 5).$$

Una vez que hayamos encontrado todas las raíces, y hayamos dividido por los correspondientes factores, nos toca buscar divisores irreducibles de grado 2, continuar con divisores irreducibles de grado 3 y así sucesivamente. Para esto, nos vendría bien tener una lista de estos polinomios irreducibles (de la misma forma que tenemos una lista $2, 3, 5, 7, 11, \cdots$ de los números primos a la que recurrimos cuando queremos factorizar un número entero).

A continuación vamos a dar una lista con los polinomios irreducibles mónicos de grados bajos en $\mathbb{Z}_p[x]$ para valores pequeños de p.

1. **Polinomios irreducibles de** $\mathbb{Z}_2[x]$**.**

   - Grado 1. Aquí, los irreducibles son todos, es decir,

     $$x \qquad x + 1.$$

   - Grado 2. Los no irreducibles son x^2, $x(x + 1) = x^2 + x$ y $(x + 1)(x + 1) = x^2 + 1$. El único que queda es

     $$x^2 + x + 1.$$

- Grado 3. También aquí los únicos que hay son los que no tienen raíces. Estos son:

$$x^3+x+1 \qquad x^3+x^2+1.$$

- Grado 4. Aquí hemos de eliminar todos los que tengan raíces y $(x^2+x+1)^2 = x^4+x^2+1$. Nos quedan entonces tres polinomios, que son:

$$x^4+x+1 \qquad x^4+x^3+1 \qquad x^4+x^3+x^2+x+1.$$

- Grado 5. Los reducibles son los que tienen raíces y los dos que toman una factorización de la forma (grado 2) $\cdot$ (grado 3). Estos dos son $(x^2+x+1)(x^3+x+1) = x^5+x^4+1$ y $(x^2+x+1)(x^3+x^2+1) = x^5+x+1$.
  Nos quedan entonces 6 polinomios que son:

$$x^5+x^2+1 \qquad x^5+x^3+1 \qquad x^5+x^4+x^3+x^2+1 \qquad x^5+x^4+x^3+x+1$$
$$x^5+x^4+x^2+x+1 \qquad\qquad x^5+x^3+x^2+x+1.$$

2. **Polinomios mónicos irreducibles en $\mathbb{Z}_3[x]$.**

- Grado 1. Al igual que antes, todos son irreducibles. Tenemos por tanto

$$x \qquad x+1 \qquad x+2.$$

- Grado 2. Son aquellos que no tiene raíces. Hay un total de 3, que son:

$$x^2+1 \qquad x^2+x+2 \qquad x^2+2x+2.$$

- Grado 3. Son también los que no tienen raíces. En este caso hay 8.

$$x^3+2x+1 \qquad x^3+2x+2 \qquad x^3+x^2+2 \qquad x^3+2x^2+1$$
$$x^3+x^2+x+2 \qquad x^3+x^2+2x+1 \qquad x^3+2x^2+x+1 \qquad x^3+2x^2+2x+2.$$

- De grado 4 hay 18 polinomios irreducibles.

3. **Polinomios mónicos irreducibles en $\mathbb{Z}_5[x]$.**

- Grado 1. Tenemos 5 irreducibles:

$$x \qquad x+1 \qquad x+2 \qquad x+3 \qquad x+4.$$

- Grado 2. Los que no tienen raíces son 10.

$$x^2+2 \qquad x^2+3 \qquad x^2+x+1 \qquad x^2+x+2 \qquad x^2+2x+3$$
$$x^2+2x+4 \qquad x^2+3x+3 \qquad x^2+3x+4 \qquad x^2+4x+1 \qquad x^2+4x+2.$$

- Para grados mayores el número de polinomios es muy grande. Así, de grado 3 la lista tendría 40 polinomios, mientras que la de grado 4 sería de 150.

4. **Polinomios mónicos irreducibles en $\mathbb{Z}_7[x]$.**

- Grado 1. Como siempre aquí son todos irreducibles.

$$x \qquad x+1 \qquad x+2 \qquad x+3 \qquad x+4 \qquad x+5 \qquad x+6.$$

- Grado 2. Aquí la lista es ya muy grande. Tenemos un total de 21 polinomios.

$$x^2+1 \quad x^2+2 \quad x^2+4 \quad x^2+x+3 \quad x^2+x+4 \quad x^2+x+6 \quad x^2+2x+2$$
$$x^2+2x+3 \quad x^2+2x+5 \quad x^2+3x+1 \quad x^2+3x+5 \quad x^2+3x+6 \quad x^2+4x+1 \quad x^2+4x+5$$
$$x^2+4x+6 \quad x^2+5x+2 \quad x^2+5x+3 \quad x^2+5x+5 \quad x^2+6x+3 \quad x^2+6x+4 \quad x^2+6x+6.$$

- De grado 3 hay un total de 112 polinomios irreducibles.

Ejemplo 3.3.3.

1. *Sea* $q(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$.

   En primer lugar, buscamos divisores de grado 1. Esto, es equivalente a buscar raíces. En este caso, puesto que $q(0) = q(1) = 1$*, el polinomio no tiene ningún divisor de grado* 1.

   Continuamos buscando divisores de grado 2. El único irreducible de grado 2 es x^2+x+1*. Probamos a dividir entonces* $q(x)$ *por* $x^2 + x + 1$*, y nos queda que* $x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$*. Los dos polinomios que aparecen son irreducibles (pues no tienen raíces).*

2. *Sea* $q(x) = x^7 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$*. Entonces:*

   Evaluamos en $x = 0$ *y* $x = 1$*. En ambos casos nos sale* 1*, luego* $q(x)$ *no tiene divisores de grado* 1.

   Dividimos por x^2+x+1*, y nos queda* $q(x) = (x^2+x+1)(x^5+x^4+x+1)+x$*. Por tanto no tiene divisores de grado* 2.

   Dividimos por $x^3 + x + 1$ *y* $x^3 + x^2 + 1$*. En el primer caso nos queda* $q(x) = (x^3 + x + 1)(x^4 + x^2) + (x^2 + x + 1)$ *y en el segundo* $q(x) = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + x + 1)$.

   Puesto que $x^4 + x^3 + x^2 + x + 1$ *no tiene divisores de grado* 1 *y grado* 2 *(ya que de tenerlos serían también divisores de* $q(x)$ *deducimos que* $x^4 + x^3 + x^2 + x + 1$ *es irreducible.*

   La factorización de $q(x)$ *como producto de irreducibles es*

   $$x^7 + x^4 + x^3 + x + 1 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + x + 1).$$

3. *Sea* $p(x) = x^7 + 2x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$*. Vamos a factorizar este polinomio como producto de irreducibles.*

   - *Buscamos los divisores de grado 1. Para esto, realizamos las divisiones según el algoritmo de Horner:*

	1	0	0	0	2	1	0	2
1		1	1	1	1	0	1	1
	1	1	1	1	0	1	1	0
1		1	2	0	1	1	2	
	1	2	0	1	1	2	0	
1		1	0	0	1	2		
	1	0	0	1	2	1		

   Vemos que nos ha salido dos veces el factor $(x - 1) = (x + 2)$*, por lo que tenemos que* $q(x) = (x + 2)^2(x^5 + 2x^4 + x^2 + x + 2)$.
   Comprobamos si el último polinomio tiene a $x = 2$ *como raíz:*

	1	2	0	1	1	2
2		2	2	1	1	1
	1	1	2	2	2	0
2		2	0	1	0	
	1	0	2	0	2	

   Es decir, el polinomio $x^5 + 2x^4 + x^2 + x + 2$ *tiene a* $x = 2$ *como una raíz simple. Tenemos ahora la factorización*

   $$q(x) = (x + 2)^2(x + 1)(x^4 + x^3 + 2x^2 + 2x + 2)$$

   Y ya hemos terminado con los divisores de grado uno.

Buscamos ahora los divisores irreducibles de grado 2, pero ya lo hacemos con el polinomio $x^4+x^3+2x^2+2x+2$. Como los únicos irreducibles de grado 2 en $\mathbb{Z}_3[x]$ son x^2+1, x^2+x+2 y x^2+2x+2, realizamos las correspondientes divisiones:

$$\begin{array}{rcrcrcr} x^4+x^3+2x^2+2x+2 & = & (x^2+1) & \cdot & (x^2+x+1) & + & x+1 \\ x^4+x^3+2x^2+2x+2 & = & (x^2+x+2) & \cdot & (x^2) & + & 2x+2 \\ x^4+x^3+2x^2+2x+2 & = & (x^2+2x+2) & \cdot & (x^2+2x+2) & + & 1 \end{array}$$

y vemos como los restos son, respectivamente, $x+1$, $2x+2$ y 1. Por tanto, el polinomio $x^4+x^3+2x^2+2x+2$ no tiene divisores de grado 2.

Como el polinomio tiene grado cuatro, y no tiene divisores de grado 1 ni de grado 2 es irreducible.

La factorización de $p(x)$ como producto de irreducibles es:

$$x^7+2x^3+x^2+2=(x+1)\cdot(x+2)^2\cdot(x^4+x^3+2x^2+2x+2)$$

3.4. Anillos cocientes de polinomios. Cuerpos finitos

En los capítulos anteriores, dado un número natural $n\geq 2$, construimos el conjunto $\mathbb{Z}_n$, y después definimos su aritmética.

Ahora, sustituimos $\mathbb{Z}$ por $\mathbb{Z}_o[x]$, con p un número. Si $m(x)\in\mathbb{Z}_p[x]$ vamos a definir el conjunto $\mathbb{Z}_p[x]_{m(x)}$. Para esto, necesitamos definir la relación de congruencia entre polinomios, de forma análoga a como se hizo con números enteros.

Definición 54. *Sea p un número primo y $a(x),b(x),m(x)\in\mathbb{Z}_p[x]$. Se dice que $a(x)$ es congruente con $b(x)$ módulo $m(x)$, y se escribe $a(x)\equiv b(x)(mód\ m(x))$ si $m(x)|(b(x)-a(x))$. Es decir:*

$$a(x)\equiv b(x)(mód\ m(x))\ \textit{si existe}\ c(x)\in\mathbb{Z}_p[x]\ \textit{tal que}\ b(x)-a(x)=c(x)m(x).$$

Nótese que la relación de congruencia módulo 0 es la relación de igualdad ($a(x)\equiv b(x)$(mód 0) si, y sólo si, $a(x)=b(x)$), mientras que si $\lambda\in\mathbb{Z}_p^*$ entonces $a(x)\equiv b(x)$(mód λ) cualesquiera que sean $a(x)$ y $b(x)$. Por tanto, nos centraremos en congruencias módulo $m(x)$ con $m(x)$ un polinomio de grado mayor o igual que 1.

Además, se tiene que $a(x)\equiv b(x)$(mód $m(x)$) si, y sólo si, $a(x)\equiv b(x)$(mód $\lambda\cdot m(x)$), donde $\lambda\in K^*$. Por tanto, al hablar de congruencias módulo $m(x)$ podemos suponer que $m(x)$ es un polinomio mónico.

Ejemplo 3.4.1. *Sea $m(x)=x^2+2\in\mathbb{Z}_3[x]$. Entonces:*

$x^4+2x^3+x^2+x+2\equiv 2x^4+x^3+2x^2+2x(mód\ x^2+2)$

pues $(2x^4+x^3+2x^2+2x)-(x^4+2x^3+x^2+x+2)=(x^2+2)(x^2+2x+2)$.

$x^4+x^3+2x^2+1\not\equiv x^3+x+2(mód\ x^2+2)$

ya que $(x^3+x+2)-(x^4+x^3+2x^2+1)=2x^2(x^2+2)+(x+1)$.

Proposición 3.4.1. *Sea $m(x)\in\mathbb{Z}_p[x]$. Entonces la relación de congruencia módulo $m(x)$ es una relación de equivalencia.*

La demostración es igual a la que se hizo para congruencias en $\mathbb{Z}$.

Para cada $m(x)\in\mathbb{Z}_p[x]$ vamos a denotar por $\mathbb{Z}_p[x]_{m(x)}$ al conjunto cociente de $\mathbb{Z}_p[x]$ por la relación de congruencia módulo $m(x)$. A la clase de equivalencia de un polinomio $a(x)$ la denotaremos inicialmente por $[a(x)]_{m(x)}$, o simplemente $[a(x)]$.

Al igual que en el caso de los números enteros, se tiene que $a(x) \equiv b(x)(\text{mód } m(x))$ si, y sólo si, $a(x)$ mód $m(x) = b(x)$ mód $m(x)$ (es decir, dan el mismo resto al dividir por $m(x)$). A partir de aquí puede verse que el conjunto $\mathbb{Z}_p[x]_{m(x)}$ está en biyección con los polinomios de $\mathbb{Z}_p[x]$ de grado menor que el de $m(x)$, pues hay tantos elementos como posibles restos de la división por $m(x)$.

Ejemplo 3.4.2.

1. *Vamos a calcular los elementos del conjunto* $\mathbb{Z}_2[x]_{(x^2+1)}$.

   Sea $p(x) \in \mathbb{Z}_2[x]$. *Al dividir* $p(x)$ *entre* x^2+1, *el resto es un polinomio de grado menor que 2 o es el polinomio nulo. Por tanto, sólo tenemos cuatro posibles restos, que son* 0, 1, x *y* $x+1$. *Tenemos entonces que*

   $$\mathbb{Z}_2[x]_{x^2+1} = \{[0], [1], [x], [x+1]\}.$$

   En la clase de equivalencia $[0]$ *están todos los polinomios que dan resto cero al dividir por* x^2+1, *es decir, todos los múltiplos de* x^2+1, *por ejemplo,* 0, x^2+1, x^3+x, x^4+1, *etc.; en la clase* $[1]$ *están los polinomios que al dividir por* x^2+1 *dan resto* 1, *como por ejemplo,* 1, x^2, x^3+x+1, x^4, *etc.*

   En resumen, se tiene:

   $$[0] = \{0,\ x^2+1,\ x^3+x,\ x^3+x^2+x+1,\ x^4+x^2,\ x^4+1, x^4+x^3+x^2+x,\ x^4+x^3+x+1, \cdots\}.$$
   $$[1] = \{1,\ x^2,\ x^3+x+1,\ x^3+x^2+x,\ x^4+x^2+1,\ x^4,\ x^4+x^3+x^2+x+1,\ x^4+x^3+x, \cdots\}.$$
   $$[x] = \{x,\ x^2+x+1,\ x^3,\ x^3+x^2+1,\ x^4+x^2+x,\ x^4+x+1,\ x^4+x^3+x^2,\ x^4+x^3+1, \cdots\}.$$
   $$[x+1] = \{x+1,\ x^2+x,\ x^3+1,\ x^3+x^2,\ x^4+x^2+x+1,\ x^4+x,\ x^4+x^3+x^2+1,\ x^4+x^3, \cdots\}.$$

   O si queremos,

   $$[0] = (x^2+1)\mathbb{Z}_2[x]; \qquad [1] = 1 + (x^2+1)\mathbb{Z}_2[x];$$
   $$(x] = x + (x^2+1)\mathbb{Z}_2[x]; \qquad [x+1] = x+1 + (x^2+1)\mathbb{Z}_2[x].$$

   Y por ejemplo, se tiene que $x^8+x^7+x^6+x+1 \in [1]$, *ya que*

   $$x^8+x^7+x^6+x+1 = 1 + (x^2+1)\cdot(x^6+x^5+x^3+x).$$

2. *El conjunto* $\mathbb{Z}_2[x]_{x^2+x+1}$ *tiene también cuatro elementos, que son* $[0]$, $[1]$, $[x]$ *y* $[x+1]$. *Sin embargo, aunque se representen igual que los de* $\mathbb{Z}_2[x]_{x^2+1}$, *los conjuntos* $\mathbb{Z}_2[x]_{x^2+x+1}$ *y* $\mathbb{Z}_2[x]_{x^2+1}$ *son distintos, pues en cada uno* $[0]$, $[1]$, $[x]$ *y* $[x+1]$ *representa cosas diferentes. Veámoslo.*

   $$[0] = \{0,\ x^2+x+1,\ x^3+x^2+x,\ x^3+1,\ x^4+x^3+x^2,\ x^4+x^3+x+1,\ x^4+x,\ x^4+x^2+1, \cdots\}.$$
   $$[1] = \{1,\ x^2+x,\ x^3+x^2+x+1,\ x^3,\ x^4+x^3+x^2+1,\ x^4+x^3+x,\ x^4+x+1,\ x^4+x^2, \cdots\}.$$
   $$[x] = \{0,\ x^2+1,\ x^3+x^2,\ x^3+x+1,\ x^4+x^3+x^2+x,\ x^4+x^3+1,\ x^4,\ x^4+x^2+x+1, \cdots\}.$$
   $$[x+1] = \{0,\ x^2,\ x^3+x^2+1,\ x^3+x,\ x^4+x^3+x^2+x+1,\ x^4+x^3,\ x^4+1,\ x^4+x^2+x, \cdots\}.$$

   Y vemos como, por ejemplo, en el primer caso, es decir, $\mathbb{Z}_2[x]_{x^2+1}$ *se tiene que* $x^3 \in [x]$ *(o* $[x^3] = [x]$*), mientras que en el segundo caso, es decir,* $\mathbb{Z}_2[x]_{x^2+x+1}$ *se tiene que* $x^3 \in [1]$.

3. *El conjunto* $\mathbb{Z}_2[x]_{x^3+x^2+x+1}$ *tiene ocho elementos, mientras que* $\mathbb{Z}_3[x]_{x^2+1}$ *tiene nueve. Determínalos en ambos casos.*

Lema 3.4.1. *Sean* $a(x), b(x), c(x), d(x), m(x) \in \mathbb{Z}_p[x]$. *Entonces:*

1. $\left.\begin{array}{l} a(x) \equiv c(x)(\text{mód } m(x)) \\ b(x) \equiv d(x)(\text{mód } m(x)) \end{array}\right\} \Longrightarrow a(x)+b(x) \equiv c(x)+d(x)(\text{mód } m(x)).$

2. $\left.\begin{array}{l} a(x) \equiv c(x)(\text{mód } m(x)) \\ b(x) \equiv d(x)(\text{mód } m(x)) \end{array}\right\} \Longrightarrow a(x)b(x) \equiv c(x)d(x)(\text{mód } m(x)).$

Y con este lema podemos ya definir las operaciones suma y producto

Definición 55. *Sean $a(x), b(x) \in \mathbb{Z}_p[x]$ y $m(x) \in \mathbb{Z}_p[x]$ mónico y no constante. Se definen en $\mathbb{Z}_p[x]_{m(x)}$ las operaciones:*

$$[a(x)] + [b(x)] = [a(x) + b(x)], \qquad [a(x)][b(x)] = [a(x)b(x)].$$

Como era de esperar, la definición hecha no depende de los representantes elegidos, y eso es consecuencia del lema 3.4.1

Ejemplo 3.4.3.

1. *Supongamos que estamos trabajando en $\mathbb{Z}_3[x]_{x^2+1}$.*

   $[x+2] + [x+1] = [2x]$.

   $[x+2][x+1] = [x^2+2] = [1]$.

   Puesto que $[x+2] = [x^2+x]$ y $[x+1] = [2x^2+x]$ podíamos haber efectuado las operaciones anteriores

   $[x^2+x] + [2x^2+x] = [3x^2+2x] = [2x]$.

   $[x^2+x][2x^2+x] = [2x^4+x^2] = [1]$, *ya que* $2x^4 + x^2 = (x^2+1)(2x^2+2) + 1$.

   Y los resultados coinciden, como no podía ser de otra forma.

2. *Vamos a fijarnos ahora en las clases de equivalencia que hemos obtenido en el ejemplo 3.4.2. En ese ejemplo, calculamos las clases de equivalencia que determinanban el conjunto $\mathbb{Z}_2[x]_{x^2+1}$ y las que determinaban el conjunto $\mathbb{Z}_2[x]_{x^2+x+1}$.*

   Vamos a sumar un elemento cualquiera de $[1]$ con un elemento cualquiera de $[x]$. El resultado va a ser un elemento de $[x+1]$. Lo vamos a hacer cuatro veces.

   - *Primero lo vamos a hacer con clases de $\mathbb{Z}_2[x]_{x^2+1}$.*

     $1 + x = x + 1 \in [x+1]$ $\qquad$ $(x^3+x^2+x) + (x^2+x+1) = x^3 + 1 \in [x+1]$

     $x^2 + (x^4+x^3+x^2) = x^4 + x^3 \in [x+1]$ $\qquad$ $(x^4+x^3+x) + (x^4+x^3+x^2) = x^2 + x \in [x+1]$.

     Y así para cualesquiera dos polinomios que tomemos, el primero perteneciente a $[1]$ y el segundo a $[x]$.

   - *Ahora lo hacemos en $\mathbb{Z}_2[x]_{x^2+x+1}$.*

     $(x^2+x) + (x^2+1) = x + 1 \in [x+1]$ $\qquad$ $x^3 + (x^4+x^3+1) = x^4 + 1 \in [x+1]$

     $(x^4+x^3+x) + (x^3+x+1) = x^4 + 1 \in [x+1]$ $\qquad$ $(x^4+x^2) + x^4 = x^2 \in [x+1]$.

De ahora en adelante, si $a \in K \subseteq \mathbb{Z}_p[x]$, denotaremos por a a la clase de equivalencia $[a] \in \mathbb{Z}_p[x]_{m(x)}$, mientras que a la clase de equivalencia $[x]$ la denotaremos por α o simplemente por x.

Nótese que siguiendo la notación $\alpha = [x]$, dado $a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$ el elemento $[a_k x^k + \cdots + a_1 x + a_0]$ se representa como $a_k \alpha^k + \cdots + a_1 \alpha + a_0$. Dicho de otra forma, $[p(x)]$ se representa como $p(\alpha)$.

Nótese también que con esta notación se verifica que $m(\alpha) = 0$, pues $m(\alpha) = [m(x)] = [0]$. Además, esta condición es suficiente para realizar las operaciones en $\mathbb{Z}_p[x]_{m(x)}$

$$\mathbb{Z}_p[x]_{m(x)} = \{p(\alpha) : p(x) \in \mathbb{Z}_p[x]; m(\alpha) = 0\}.$$

Ejemplo 3.4.4.

1. *En el conjunto $\mathbb{Z}_2[x]_{x^3+x+1}$ vamos a multiplicar $[x^2+x+1]$ y $[x^2+1]$. Podemos proceder de dos formas:*

a) *Multiplicamos los dos polinomios:*
$[x^2+x+1][x^2+1]=[x^4+x^3+x+1]$.
Dividimos x^4+x^3+x+1 *entre* x^3+x+1. $x^4+x^3+x+1=(x^3+x+1)(x+1)+x^2+x$.
Por tanto $[x^2+x+1][x^2+1]=[x^2+x]$.

b) $(\alpha^2+\alpha+1)(\alpha^2+1)=\alpha^4+\alpha^3+\alpha+1$.
Puesto que $\alpha^3+\alpha+1=0$ *deducimos que* $\alpha^3=\alpha+1$, *luego* $\alpha^4=\alpha^2+\alpha$. *Por tanto* $(\alpha^2+\alpha+1)(\alpha^2+1)=\alpha^4+\alpha^3+\alpha+1=(\alpha^2+\alpha)+(\alpha+1)+\alpha+1=\alpha^2+\alpha$.

En los dos casos se obtiene el mismo resultado.

2. $\mathbb{Z}_2[x]_{x^2+1}=\{0,1,\alpha,\alpha+1:\alpha^2+1=0\}$, *o si preferimos:*

$$\mathbb{Z}_2[x]_{x^2+1}=\{0,1,\alpha,\alpha+1:\alpha^2=1\}.$$

Proposición 3.4.2. *Sea* $m(x)\in\mathbb{Z}_p[x]$ *mónico y no constante. Las operaciones suma y producto en* $\mathbb{Z}_p[x]_{m(x)}$ *verifican las siguientes propiedades (aquí vamos a denotar a* $[x]$ *por* x*):*

i) $p(x)+(q(x)+r(x))=(p(x)+q(x))+r(x)$

ii) $p(x)+q(x)=q(x)+p(x)$

iii) $p(x)+0=p(x)$

iv) Para cada $p(x)\in\mathbb{Z}_p[x]_{m(x)}$ *existe* $q(x)\in\mathbb{Z}_p[x]_{m(x)}$ *tal que* $p(x)+q(x)=0$.

v) $p(x)(q(x)r(x))=(p(x)q(x))r(x)$

vi) $p(x)q(x)=q(x)p(x)$

vii) $p(x)\cdot 1=p(x)$

viii) $p(x)(q(x)+r(x))=p(x)q(x)+p(x)r(x)$

Estas propiedades nos dicen que $\mathbb{Z}_p[x]_{m(x)}$ es un anillo conmutativo.

Ejemplo 3.4.5.

1. *Consideramos el anillo* $\mathbb{Z}_2[x]_{x^3+1}$. *Vamos a escribir las tablas de sumar y multiplicar de dicho anillo. Antes de ello, enumeramos sus elementos*

$$\mathbb{Z}_2[x]_{x^3+1}=\{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$$

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

Para realizar la tabla del producto tenemos en cuenta que $\alpha^3+1=0$, *es decir,* $\alpha^3=1$.

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	1	$\alpha+1$	α^2+1	$\alpha^2+\alpha+1$
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2+1	$\alpha^2+\alpha$	$\alpha+1$	0
α^2	0	α^2	1	α^2+1	α	$\alpha^2+\alpha$	$\alpha+1$	$\alpha^2+\alpha+1$
α^2+1	0	α^2+1	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha+1$	α^2+1	0
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	α^2+1	$\alpha+1$	$\alpha+1$	α^2+1	$\alpha^2+\alpha$	0
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	0	0	$\alpha^2+\alpha+1$

Donde algunas de las celdas se han completado como sigue:

$$\alpha\cdot\alpha^2=\alpha^3=1$$

$$(\alpha^2+1)(\alpha^2+\alpha+1)=\alpha^4+\alpha^3+\alpha^2+\alpha^2+\alpha+1=\alpha+1+\alpha^2+\alpha^2+\alpha+1=0$$

Y se ha tenido en cuenta que $\alpha^4=\alpha^3\cdot\alpha=\alpha$.

$$(\alpha^2+1)(\alpha^2+1)=\alpha^4+2\alpha^2+1=\alpha+1.$$

2. *Vamos a dar ahora la tabla de multiplicar de* $\mathbb{Z}_3[x]_{x^2+1}$. *Los elementos son ahora*

$$\mathbb{Z}_3[x]_{x^2+1}=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$$

$\cdot$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	2	$\alpha+2$	$2\alpha+2$	1	$\alpha+1$	$2\alpha+1$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$\alpha+2$	2α	1	$2\alpha+1$	2	α
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	1	α	$\alpha+1$	2α	2
2α	0	2α	α	1	$2\alpha+1$	$\alpha+1$	2	$2\alpha+2$	$\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$\alpha+1$	2	2α	$2\alpha+2$	α	1
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$2\alpha+1$	α	2	$\alpha+2$	1	2α

Proposición 3.4.3. *Sea* p *un número primo,* $m(x)\in\mathbb{Z}_p[x]$ *no constante y* $q(\alpha)\in\mathbb{Z}_p[x]_{m(x)}$. *Entonces:*

- $q(\alpha)$ *es una unidad si, y sólo si,* $mcd(q(x),m(x))=1$.
- $q(\alpha)$ *es un divisor de cero si, y sólo si,* $mcd(q(x),m(x))\neq 1$.

Recordemos que si A es un anillo conmutativo, un elemento $a\in A$ se dice unidad si existe $b\in A$ tal que $a\cdot b=1$, mientras que se dice divisor de cero si existe $b\neq 0$ tal que $a\cdot b=0$.

Demostración: La demostración de la primera parte es análoga a la demostración de la proposición 2.5.2

En cuanto a la segunda, si $p(\alpha)$ es un divisor de cero, entonces $p(\alpha)$ no es una unidad (¿por qué?), luego $mcd(p(x),m(x))\neq 1$.

Recíprocamente, si $mcd(p(x),m(x))\neq 1$, consideramos $q(x)=\frac{m(x)}{d(x)}$ donde $d(x)=mcd(p(x),m(x))$. Entonces $gr(q(x))<gr(m(x))$, lo que implica que $q(\alpha)\neq 0$, y puesto que $p(x)q(x)$ es múltiplo de $m(x)$ ya que

$$p(x)q(x)=p(x)\frac{m(x)}{d(x)}=\frac{p(x)}{d(x)}m(x)$$

se verifica que $p(\alpha)q(\alpha)=0$. ■

Ejemplo 3.4.6. *En $\mathbb{Z}_2[x]$ se verifica que $mcd(x^2+1, x^3+1) = x+1$. Por tanto, α^2+1 es un divisor de cero en $\mathbb{Z}_2[x]_{x^3+1}$. Además, para encontrar un elemento que al multiplicarlo por él nos de cero, calculamos $\frac{x^3+1}{x+1}$. Ese cociente vale x^2+x+1. Deducimos entonces que $(\alpha^2+1)(\alpha^2+\alpha+1) = 0$, como podemos ver en el ejemplo anterior.*

A partir de la proposición anterior se deduce fácilmente que si $m(x)$ es un polinomio irreducible en $\mathbb{Z}_p[x]$, entonces $\mathbb{Z}_p[x]_{m(x)}$ es un cuerpo. Si $m(x)$ es un polinomio irreducible de grado n en $\mathbb{Z}_p[x]$ entonces $\mathbb{Z}_p[x]_{m(x)}$ es un cuerpo con p^n elementos.

Por otra parte, si K es un cuerpo con un número finito de elementos, entonces su característica es un número primo p[1] En tal caso se tiene que $\mathbb{Z}_p \subseteq K$. Utilizando resultados de álgebra lineal se puede ver que existe un número natural n de forma que K tiene p^n elementos.

Es decir, por una parte hemos visto que el número de elementos de un cuerpo finito es una potencia de un primo. Por otra parte, hemos visto como, dado un número primo p y un número natural n podemos construir un cuerpo con p^n elementos. Basta encontrar un polinomio irreducible de grado n en $\mathbb{Z}_p[x]$. Hay un teorema que nos asegura la existencia de polinomios irreducibles de cualquier grado en $\mathbb{Z}_p[x]$.

La existencia de varios polinomios irreducibles de un mismo grado en $\mathbb{Z}_p[x]$ daría lugar, en principio, a distintos cuerpos con p^n elementos. Sin embargo, todos los cuerpos con el mismo cardinal son isomorfos, en el sentido que vamos a explicar a continuación.

Ejemplo 3.4.7.

1. *Hemos visto que $\mathbb{Z}_3[x]_{x^2+1}$ es un cuerpo con nueve elementos, cuya tabla del producto calculamos en el ejemplo 3.4.5. Puesto que x^2+x+2 es también un polinomio irreducible en $\mathbb{Z}_3[x]$ tenemos que $\mathbb{Z}_3[x]_{x^2+x+2}$ es también un cuerpo con nueve elementos. Si llamamos β al elemento $[x]$, entonces la tabla del producto de este cuerpo es:*

$(\mathbb{Z}_3[x]_{x^2+x+2}, \cdot)$	0	1	2	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$
2	0	2	1	2β	$2\beta+2$	$2\beta+1$	β	$\beta+2$	$\beta+1$
β	0	β	2β	$2\beta+1$	1	$\beta+1$	$\beta+2$	$2\beta+2$	2
$\beta+1$	0	$\beta+1$	$2\beta+2$	1	$\beta+2$	2β	2	β	$2\beta+1$
$\beta+2$	0	$\beta+2$	$2\beta+1$	$\beta+1$	2β	2	$2\beta+2$	1	β
2β	0	2β	β	$\beta+2$	2	$2\beta+2$	$2\beta+1$	$\beta+1$	1
$2\beta+1$	0	$2\beta+1$	$\beta+2$	$2\beta+2$	β	1	$\beta+1$	2	2β
$2\beta+2$	0	$2\beta+2$	$\beta+1$	2	$2\beta+1$	β	1	2β	$\beta+2$

donde se ha usado que $\beta^2 = 2\beta+1$, relación que se deduce de $\beta^2+\beta+2 = 0$ (es decir, $m(\beta) = 0$). Si ahora hacemos el cambio $\alpha = \beta+2$, es decir, $\beta = \alpha+1$, la tabla nos quedaría

$(\mathbb{Z}_3[x]_{x^2+x+2}, \cdot)$	0	1	2	$\alpha+1$	$\alpha+2$	α	$2\alpha+2$	2α	$2\alpha+1$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$\alpha+1$	$\alpha+2$	α	$2\alpha+2$	2α	$2\alpha+1$
2	0	2	1	$2\alpha+2$	$2\alpha+1$	2α	$\alpha+1$	α	$\alpha+2$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	2α	1	$\alpha+2$	α	$2\alpha+1$	2
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	1	α	$2\alpha+2$	2	$\alpha+1$	2α
α	0	α	2α	$\alpha+2$	$2\alpha+2$	2	$2\alpha+1$	1	$\alpha+1$
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	α	2	$2\alpha+1$	2α	$\alpha+2$	1
2α	0	2α	α	$2\alpha+1$	$\alpha+1$	1	$\alpha+2$	2	$2\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	2	2α	$\alpha+1$	1	$2\alpha+2$	α

[1]la característica de un anillo A se define como el menor número natural m tal que $1+1+\overset{m \text{ veces}}{\cdots}+1 = 0$, si dicho número existe.

Si comparamos esta tabla con la que obtuvimos para $\mathbb{Z}_3[x]_{x^2+1}$ vemos que es exactamente la misma (salvo el orden de las filas y columnas). Vemos entonces que los cuerpos $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_3[x]_{x^2+x+2}$ son iguales, o más precisamente, son isomorfos.

De hecho, lo único que diferencia a los cuerpos $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_3[x]_{x^2+x+2}$ es, aparte del camino para obtenerlos, el nombre que se le ha dado a los elementos. Lo que en un cuerpo se llama α en el otro se llama $\beta+2$. Una vez hecha la correcta correspondencia entre los elementos de uno y del otro, se opera de igual forma en un caso y en el otro.

Nota: *Dados dos cuerpos K y K', se dice que son isomorfos si existe una aplicación $f : K \to K'$ satisfaciendo:*

a) *f preserva la suma, es decir, $f(a+b) = f(a) + f(b)$.*
b) *f preserva el producto, es decir, $f(ab) = f(a)f(b)$.*
c) *f es biyectiva.*

f es lo que se llama un isomorfismo de cuerpos.
En el caso de $K = \mathbb{Z}_3[x]_{x^2+x+2}$ y $K' = \mathbb{Z}_3[x]_{x^2+1}$, la aplicación $f : K \to K'$ dada por

$$0 \mapsto 0 \quad 1 \mapsto 1 \quad 2 \mapsto 2 \quad \beta \mapsto \alpha + 1 \quad \beta + 1 \mapsto \alpha + 2$$

$$\beta + 2 \mapsto \alpha \quad 2\beta \mapsto 2\alpha + 2 \quad 2\beta + 1 \mapsto 2\alpha \quad 2\beta + 2 \mapsto 2\alpha + 1$$

es un isomorfismo de cuerpos. Obviamente, este isomorfismo queda totalmente determinado por $\beta \mapsto \alpha + 1$.

Nota:

Aunque en la última sección nos hemos centrado en el caso de polinomios con coeficientes en $\mathbb{Z}_p$, todo el desarrollo podría haberse hecho para el caso de polinomios con coeficientes en un cuerpo cualquiera.

Vamos a tomar como cuerpo K el conjunto de los números reales, y $m(x) = x^2+1$. Este polinomio es irreducible (tiene grado 2 y no tiene raíces), luego $\mathbb{R}[x]_{x^2+1}$ es un cuerpo.

Vamos a denotar por i a $[x]$ (en lugar de α). Entonces, los elementos de $\mathbb{R}[x]_{x^2+1}$ son de la forma $a+bi$, donde $a, b \in \mathbb{R}$. Además, $i^2 + 1 = 0$, es decir, $i^2 = -1$.

Por tanto,

$$\mathbb{R}[x]_{x^2+1} = \{a + bi : a, b \in \mathbb{R}; i^2 = -1\}$$

luego el cuerpo obtenido resulta ser igual (o isomorfo) a $\mathbb{C}$.

Dado p es un número primo y n es un número natural no nulo, denotaremos como $\mathbb{F}_{p^n}$ al único cuerpo que existe con p^n elementos. Así, por ejemplo, $\mathbb{F}_4 = \mathbb{Z}_2[x]_{x^2+x+1}$ y $\mathbb{F}_9 = \mathbb{Z}_3[x]_{x^2+1}$. Obviamente, $\mathbb{F}_p = \mathbb{Z}_p$ para cualquier primo p.

Capítulo 3

El anillo de polinomios sobre un cuerpo

3.1. Generalidades sobre polinomios

Definición 37. *Sea A un anillo conmutativo, y x un elemento que no pertenece a A. Un polinomio con coeficientes en A es una expresión de la forma*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

donde $n \in \mathbb{N}$ y $a_k \in A$.

> **Nota:** Recordemos que un anillo conmutativo es un conjunto A en el que hay definidas dos operaciones, $+$ y $\cdot$ (suma y producto), que son asociativas, conmutativas y tienen elemento neutro (0 para la suma y 1 para el producto), todo elemento tiene un inverso (opuesto) para la suma, y la suma es distributiva respecto al producto.
>
> Básicamente, un anillo es un conjunto en el que podemos sumar, restar y multiplicar los elementos, con las propiedades usuales de estas operaciones.
>
> Ejemplos de anillos que utilizaremos son $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_n$.

Ejemplo 3.1.1. *Son polinomios con coeficientes en $\mathbb{Z}$*

$$2x^2 + 3x + (-1); \quad 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2$$

En el primer caso $n = 2$, $a_2 = 2$, $a_1 = 3$ y $a_0 = -1$, mientras que en el segundo $n = 5$ y $a_5 = a_4 = a_3 = a_2 = a_1 = a_0 = 2$.

No son polinomios con coeficientes en $\mathbb{Z}$

$$3x^2 - x + 2 + x^{-1}; \quad sen(x) - 3$$

> **Nota:** La definición que se ha dado no es muy rigurosa. De hecho, con esa definición, la expresión $x^2 + 1$ no es un polinomio, pues no se ajusta a lo explicitado en dicha definición, ya que no está dicho quien es a_1 ni a_2. Sí es un polinomio, de acuerdo con la definición dada $1x^2 + 0x + 1$. Obviamente, al referirnos al polinomio $1x^2 + 0x + 1$ lo haremos como $x^2 + 1$. De la misma forma, el primer polinomio que aparece en el ejemplo anterior lo escribiremos $2x^2 + 3x - 1$.
>
> En general, si $a_k x^k + \cdots + a_1 x + a_0$ es un polinomio y $a_i = 0$, entonces el polinomio dado diremos que es igual a $a_k x^k + \cdots + a_{i+1} x^{i+1} + a_{i-1} x^{i-1} + \cdots + a_0$ (salvo que el polinomio de partida sea 0).
>
> Tampoco se ajusta a la definición que hemos dado de polinomio, por ejemplo, la expresión $5+2x+3x^2$. Deberíamos escribir $3x^2 + 2x + 5$.
>
> En lo que sigue no tendremos en cuenta estas deficiencias de la definición dada.

Dado un anillo A denotaremos por $A[x]$ al conjunto de todos los polinomios con coeficientes en A.

Definición 38. *Sea A un anillo.*

1. *Sean* $p(x) = a_m x^m + \cdots + a_1 x + a_0$ *y* $q(x) = b_n x^n + \cdots + b_1 x + b_0$ *dos elementos de* $A[x]$*, y supongamos que* $m \leq n$*. Se define la suma de los polinomios* $p(x)$ *y* $q(x)$ *como el polinomio*

$$p(x) + q(x) = b_n x^n + \cdots + b_{m+1} x_{m+1} + (a_m + b_m) x^m + \cdots + (a_1 + b_1) x + (a_0 + b_0)$$

2. *Sea* $k \in \mathbb{N}$*,* $p(x) = a_m x^m + \cdots + a_1 x + a_0$*,* $q(x) = b_k x^k \in A[x]$ *(si* $k = 0$ *entonces* $q(x) = b_0$*). Se define el producto de* $p(x)$ *y* $q(x)$ *como el polinomio:*

$$p(x) \cdot q(x) = a_n b_k x^{k+n} + \cdots + a_1 b_k x^{k+1} + a_0 b_k x^k$$

Sean ahora $p(x) = a_m x^m + \cdots + a_1 x + a_0$ *y* $q(x) = b_n x^n + \cdots + b_1 x + b_0$*. Se define el producto de* $p(x)$ *y* $q(x)$ *como*

$$p(x) \cdot q(x) = p(x) \cdot q_n(x) + \cdots + p(x) \cdot q_1(x) + p(x) \cdot q_0(x)$$

donde $q_k(x) = b_k x^k$*.*

Las dos operaciones definidas satisfacen las siguientes propiedades:

- La suma de polinomios es asociativa, es decir, $p(x) + (q(x) + r(x)) = p(x) + q(x)) + r(x)$. Nótese que esta propiedad es necesaria para poder definir el producto tal y como se ha hecho aquí.
- La suma de polinomios es conmutativa.
- La suma tiene un elemento neutro. Éste será denotado por 0.
- Dado $p(x) \in A[x]$ existe $q(x) \in A[x]$ tal que $p(x) + q(x) = 0$. Denotaremos como $-p(x)$ a este polinomio.
- El producto de polinomios es asociativo y conmutativo.
- El producto tiene un elemento neutro. Éste será denotado por 1.
- La suma es distributiva con respecto al producto.

Estas propiedades nos dicen que, si A es un anillo conmutativo, entonces $A[x]$ es también un anillo conmutativo.

Además, podemos identificar A como los elementos de $A[x]$ de la forma $p(x) = a$, en cuyo caso A es un subanillo de $A[x]$.

Ejemplo 3.1.2. *Sea* $A = \mathbb{Z}_{12}$*, y sean* $p(x) = 2x^3 + 3x^2 + 7x + 9$ *y* $q(x) = 6x^2 + 5x + 4$*. Entonces:*

$* \; p(x) + q(x) = 2x^3 + (3+6)x^2 + (7+5)x + (9+4) = 2x^3 + 9x^2 + 1$

$$\begin{aligned} * \; p(x) \cdot q(x) &= p(x) \cdot (6x^2) + p(x) \cdot (5x) + p(x) \cdot 4 \\ &= (0x^5 + 6x^4 + 6x^3 + 6x^2) + (10x^4 + 3x^3 + 11x^2 + 9x) + (8x^3 + 0x^2 + 4x + 0) \\ &= 4x^4 + 5x^3 + 5x^2 + x \end{aligned}$$

Normalmente, para efectuar la multiplicación dispondremos los datos de la siguiente forma:

$p(x)$			2	3	7	9
$q(x)$				6	5	4
$p(x) \cdot 4$			8	0	4	0
$p(x) \cdot 5x$		10	3	11	9	
$p(x) \cdot 6x^2$	0	6	6	6		
$p(x) \cdot q(x)$	0	4	5	5	1	0

luego el resultado final es $4x^4 + 5x^3 + 5x^2 + x$*.*

Daremos a continuación algunos conceptos referentes a los polinomios:

Definición 39. *Sea* A *un anillo conmutativo y* $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$*.*

i) Si $a_n \neq 0$ entonces se dice que el polinomio $p(x)$ tiene **grado** *n ($gr(p(x)) = n$). Nótese que no se ha definido el grado del polinomio 0. En ocasiones, consideraremos que el grado del polinomio 0 es -1.*

ii) Al elemento $a_k \in A$ se le llama **coeficiente de grado k**, *y a la expresión $a_k x^k$,* **término de grado k**.

iii) El coeficiente de grado n de un polinomio de grado n se llama **coeficiente líder**, *y a la expresión $a_n x^n$* **término líder**.

iv) El coeficiente de grado 0 de un polinomio se le llama **término independiente**.

v) Un polinomio cuyo coeficiente líder valga 1 se dice que es un **polinomio mónico**.

vi) Un polinomio que, bien tiene grado 0, o bien es el polinomio 0 se dice que es un **polinomio constante**.

Ejemplo 3.1.3. *Sean $p(x) = 3x^3+5x+2$ y $q(x) = x^4+2x^3+3x^2+5x+8$ dos polinomios con coeficientes en $\mathbb{Z}_{11}$. Entonces:*

- $gr(p(x)) = 3$ y $gr(q(x)) = 4$.

- El coeficiente de grado 2 de $p(x)$ es 0, mientras que el coeficiente de grado 2 de $q(x)$ es 3. El coeficiente de grado 5 de $q(x)$ es cero.

- El coeficiente líder de $p(x)$ es 3, mientras que el coeficiente líder de $q(x)$ es 1. Por tanto, $q(x)$ es mónico, mientras que $p(x)$ no lo es.

- Los términos independientes de $p(x)$ y $q(x)$ son 2 y 8 respectivamente.

- Ninguno de los dos polinomios son constantes.

Proposición 3.1.1. *Sean $p(x), q(x) \in A[x]$. Entonces:*

$$gr(p(x) + q(x)) \leq máx\{gr(p(x), q(x)\}$$

$$gr(p(x) \cdot q(x)) \leq gr(p(x)) + gr(q(x))$$

La demostración de ambos hechos es fácil. Podría pensarse que en el segundo caso se da siempre la igualdad ($gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$). Sin embargo, el Ejemplo 3.1.2 nos muestra un caso en el que se da la desigualdad estricta.

Es fácil comprobar que si $p(x)$ o $q(x)$ es mónico, entonces se verifica que $gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$.

Terminamos esta sección estudiando la evaluación de un polinomio en un punto.

Definición 40. *Sea A un anillo, $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$ y $a \in A$. Se define la evaluación de $p(x)$ en el punto a, $Ev_a(p(x))$ como el elemento de A:*

$$Ev_a(p(x)) = a_n a^n + \cdots + a_1 a + a_0$$

Dicho de otra forma, $Ev_a(p(x))$ es el resultado de sustituir en la expresión de $p(x)$ el símbolo x por a. De esta forma tenemos definida una aplicación (morfismo de anillos) $Ev_a : A[x] \to A$.

Normalmente, escribiremos $p(a)$ en lugar de $Ev_a(p(x))$.

Proposición 3.1.2. *Dado A un anillo y $p_1(x), p_2(x) \in A[x]$*

1. *Si $q(x) = p_1(x) + p_2(x)$ entonces $q(a) = p_1(a) + p_2(a)$ (es decir, $Ev_a(p_1(x) + p_2(x)) = Ev_a(p_1(x)) + Ev_a(p_2(x))$.*
2. *Si $q(x) = p_1(x) \cdot p_2(x)$ entonces $q(a) = p_1(a) \cdot p_2(a)$ (es decir, $Ev_a(p_1(x) \cdot p_2(x)) = Ev_a(p_1(x)) \cdot Ev_a(p_2(x))$.*

Usando la aplicación evaluación, cada polinomio de $A[x]$ determina una aplicación $A \to A$, dada por $a \mapsto p(a)$.

Ejemplo 3.1.4.

1. *El polinomio* $x^3+3x^2+2x+2 \in \mathbb{Z}_5[x]$ *determina la aplicación* $\mathbb{Z}_5 \to \mathbb{Z}_5$ *siguiente:*

$$0 \mapsto 2 \quad 1 \mapsto 3 \quad 2 \mapsto 1 \quad 3 \mapsto 2 \quad 4 \mapsto 2$$

2. *El polinomio* $x^2+x+1 \in \mathbb{Z}_2[x]$ *determina la aplicación*

$$0 \mapsto 1 \qquad 1 \mapsto 1$$

es decir, la aplicación constante 1.

3.2. Máximo común divisor y mínimo común múltiplo

Definición 41. *Sean* $p(x), q(x) \in A[x]$. *Se dice que* $p(x)$ *divide a* $q(x)$, *o que* $q(x)$ *es múltiplo de* $p(x)$, *y escribiremos* $p(x)|q(x)$, *si existe* $c(x) \in A[x]$ *verificando que* $q(x) = p(x) \cdot c(x)$.

Ejemplo 3.2.1.

1. *Sean* $p(x) = x^2-1$ *y* $q(x) = 2x+2$ *dos polinomios con coeficientes en* $\mathbb{Q}$. *Entonces* $q(x)|p(x)$, *pues* $p(x) = q(x) \cdot (\frac{1}{2}x - \frac{1}{2})$. *Sin embargo, si consideramos ambos polinomios en* $\mathbb{Z}[x]$ *entonces* $q(x)$ *no divide a* $p(x)$.
2. *En* $\mathbb{Z}_2[x]$ *se verifica que* $(x+1)|(x^2+1)$, *ya que* $x^2+1 = (x+1)(x+1)$.
3. *En* $\mathbb{Z}_3[x]$ *se verifica que* $(x+1) \not| (x^2+1)$, *pues si* $x^2+1 = (x+1) \cdot c(x)$, *entonces* $gr(c(x)) = 1$, *luego* $c(x) = c_1x + c_0$. *Operando resulta que* $c_0 = 1$, $c_0 + c_1 = 0$ *y* $c_1 = 1$, *lo cual es imposible.*
4. *En* $\mathbb{Z}_4[x]$ *se verifica que* $(x+2)|(2x^2+x+2)$, *pues* $2x^2+x+2 = (x+2)(2x+1)$ *y* $(2x^2+x+2)|(x+2)$ *pues* $x+2 = (2x^2+x+2)(2x+1)$.
5. *Para cualquier* $p(x) \in A[x]$ *se verifica que* $1|p(x)$ *y* $p(x)|0$.

En lo que sigue nos centraremos en polinomios con coeficientes en un cuerpo, o con coeficientes en $\mathbb{Z}$. Recordemos que un cuerpo es un anillo conmutativo en el que cada elemento no nulo tiene un inverso para el producto. Dicho de otra forma, es un conjunto en el que podemos sumar, restar, multiplicar y dividir (salvo por 0). Ejemplos de cuerpos son $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{Z}_p$, donde p es un número primo.

Veamos a continuación algunas propiedades referentes a la relación de divisibilidad de polinomios.

Proposición 3.2.1. *Sea* K *un cuerpo y* $p(x), q(x), r(x) \in K[x]$. *Entonces:*

1. $p(x)|p(x)$.
2. *Si* $p(x)|q(x)$ *y* $q(x)|p(x)$, *entonces existe* $a \in K^*$ *tal que* $q(x) = a \cdot p(x)$.
3. *Si* $p(x)|q(x)$ *y* $q(x)|r(x)$, *entonces* $p(x)|r(x)$.
4. *Si* $p(x)|q(x)$ *y* $p(x)|r(x)$, *entonces* $p(x)|(q(x)+r(x))$.
5. *Si* $p(x)|q(x)$, *entonces* $p(x)|q(x) \cdot r(x)$ *para cualquier* $r(x) \in K[x]$.

La demostración de estas propiedades es casi inmediata.

Si trabajamos con polinomios con coeficientes en $\mathbb{Z}$, todas las propiedades son iguales salvo la segunda. Se pide estudiar que ocurre si tenemos dos polinomios $p(x), q(x) \in \mathbb{Z}[x]$ tales que $p(x)|q(x)$ y $q(x)|p(x)$.

Los apartados 1,3,4,5 son igualmente válidos para polinomios con coeficientes en un anillo conmutativo A. El ejemplo 3.2.1.4 nos dice que el apartado 2 no es válido en general.

Antes de estudiar el máximo común divisor y el mínimo común múltiplo de dos polinomios veamos cómo dividir polinomios.

Teorema 3.2.1 (Algoritmo de la división). *Sea K un cuerpo, y $p(x), q(x)$ dos polinomios de $K[x]$, con $q(x) \neq 0$. Entonces existen únicos polinomios $c(x), r(x) \in K[x]$ tales que:*

$p(x) = q(x) \cdot c(x) + r(x)$

$r(x) = 0$ *o* $gr(r(x)) < gr(q(x))$.

Los polinomios $c(x)$ y $r(x)$ son llamados cociente y resto respectivamente.

Demostración:
Vamos a dar una indicación de como sería la demostración de existencia.
Supongamos que $gr(q(x)) = m$ y que b_m es el coeficiente líder de $q(x)$.
Distingamos dos casos:

- $gr(p(x)) < m$. En tal caso, basta tomar $c(x) = 0$ y $r(x) = p(x)$.
- $gr(p(x)) \geq m$. Llamemos entonces n al grado de $p(x)$ y sea a_n su coeficiente líder. Sea entonces $c_1(x) = a_n \cdot (b_m)^{-1} x^{n-m}$ y $p_1(x) = p(x) - q(x) \cdot c_1(x)$. Se tiene entonces que:
  - $p(x) = q(x) \cdot c_1(x) + p_1(x)$. Esto es evidente por cómo hemos definido $p_1(x)$.
  - $gr(p_1(x)) < gr(p(x))$ o $p_1(x) = 0$. Esto es así porque el término líder de $q(x) \cdot c_1(x)$ vale $-a_n x^n$. Por tanto, al hacer la resta $p(x) - q(x) \cdot c_1(x)$, el coeficiente líder de $p(x)$ se anula con el coeficiente líder de $q(x) \cdot c_1(x)$.

Si ahora $gr(p_1(x)) < m$ (o $p_1(x) = 0$), ya hemos terminado. Basta tomar $c(x) = c_1(x)$ y $r(x) = p_1(x)$. En caso contrario, repetimos con $p_1(x)$ el mismo proceso que con $p(x)$.
Obtenemos así dos polinomios $p_2(x)$ y $c_2(x)$ tales que $p_1(x) = q(x) \cdot c_2(x) + p_2(x)$ y $gr(p_2(x)) < gr(p_1(x))$ o $p_2(x) = 0$. En tal caso, se tiene que:

$$p(x) = q(x) \cdot c_1(x) + p_1(x) = q(x) \cdot c_1(x) + q(x) \cdot c_2(x) + p_2(x) = q(x) \cdot (c_1(x) + c_2(x)) + p_2(x)$$

Obtenemos así dos sucesiones de polinomios $c_1(x), c_2(x), \cdots c_k(x)$ y $p_1(x), p_2(x), \cdots, p_k(x)$ satisfaciendo

- $p(x) = q(x) \cdot (c_1(x) + c_2(x) + \cdots + c_k(x)) + p_k(x)$
- $p_k(x) = 0$ ó $gr(p_k(x)) < gr(p_{k-1}(x)) < \cdots < gr(p_1(x)) < gr(p(x))$.

Este proceso lo continuamos hasta que $gr(p_k(x))$ sea menor que m o $p_k(x)$ sea igual al polinomio cero. En tal caso, basta tomar $c(x) = c_1(x) + \cdots + c_k(x)$ y $r(x) = p_k(x)$.
La demostración de la unicidad se deja como ejercicio.
■

Nótese que si en lugar de considerar un cuerpo consideramos un anillo conmutativo cualquiera, y $p(x), q(x)$ son dos polinomios tales que el coeficiente líder de $q(x)$ es una unidad, entonces podría repetirse la demostración.
Por tanto, si $p(x), q(x) \in A[x]$ y $q(x)$ es mónico, existe únicos $c(x), r(x) \in A[x]$ tales que $p(x) = q(x) \cdot c(x) + r(x)$, y $gr(r(x)) < gr(q(x))$ o $r(x) = 0$.

Ejemplo 3.2.2. *Calculemos el cociente y el resto de la división del polinomio $p(x) = 2x^4 + 3x^3 + 5x + 1$ entre $q(x) = 3x^3 + x + 6$ en $\mathbb{Z}_7[x]$. Lo haremos siguiendo los pasos hechos en la demostración precedente.*
Notemos en primer lugar que $gr(p(x)) > gr(q(x))$.
Calculamos 3^{-1}. Se tiene que $3^{-1} = 5$.
Tomamos entonces el polinomio $c_1(x) = 2 \cdot 5 \cdot x^{4-3} = 3x$.
Hallamos $p_1(x) = p(x) - 3xq(x) = p(x) + 4xq(x) = 3x^3 + 4x^2 + x + 1$.

Dado que $gr(p_1(x)) \geq gr(q(x))$ *continuamos dividiendo. Tomamos el polinomio* $c_2(x) = 3 \cdot 5x^{3-3} = 1$
Hallamos $p_2(x) = p_1(x) - 1q(x) = p_1(x) + 6q(x) = 4x^2 + 2$.
Dado que $gr(p_2(x)) < gr(q(x))$ *la división ha terminado. El cociente es* $c(x) = c_1(x) + c_2(x) = 3x + 1$ *y el resto* $r(x) = 4x^2 + 2$.
Los cálculos podemos disponerlos como sigue:

2	3	0	5	1	|	3	0	1	6
5	0	4	3			3	1		
	3	4	1	1					
	4	0	6	1					
		4	0	2					

Si analizamos el estudio que hicimos de los números enteros, podemos ver como el algoritmo de la división resultó clave en el desarrollo posterior. A partir de él se pudo probar la existencia de máximo común divisor y calcularlo; encontrar los coeficientes de Bezout, que luego fueron la base para la resolución de congruencias.

Ahora, en $K[x]$ tenemos también un algoritmo de división, luego todo lo dicho para números enteros vale también para polinomios. En lo que sigue, trasladaremos los resultados del tema anterior al caso de los polinomios, incidiendo en las particularidades de éstos.

Nota: Un anillo A, se dice que es un dominio euclídeo si en él tenemos definida una aplicación *grado*, $g : A^* \to \mathbb{N}$ satisfaciendo dos propiedades:

- $g(ab) \geq g(a)$ para $b \neq 0$
- Para todo $a, b \in A$, $b \neq 0$, existen $q, r \in A$ tales que $a = bq + r$ y $g(r) < g(a)$ ó $r = 0$.

Es decir, un Dominio Euclídeo viene a ser un anillo en el que tenemos definida una división, con resto.

Tenemos entonces que $\mathbb{Z}$ y $K[x]$ son dominios euclídeos (las funciones grado son, en el caso de $\mathbb{Z}$ el valor absoluto, y en el caso de $K[x]$ el grado).

En un dominio euclídeo se verifica el teorema de Bezout, el teorema chino del resto, el teorema de factorización única, etc.

Definición 42. *Sean* $p(x), q(x) \in K[x]$, *con* $q(x) \neq 0$. *Se definen los polinomios* $p(x)$ *mód* $q(x)$ *y* $p(x)$ *div* $q(x)$ *como el resto y el cociente de dividir* $p(x)$ *entre* $q(x)$.
Cuando $p(x)$ *mód* $q(x) = 0$, *denotaremos por* $\frac{p(x)}{q(x)}$ *al polinomio* $p(x)$ *div* $q(x)$.

Ejemplo 3.2.3.

1. *En* $\mathbb{Z}_3[x]$, *se verifica que:*

   $x^5 + x^4 + 2x^3 + x^2 + x + 1$ *mód* $x^2 + 2x + 1 = 2$
   $x^5 + x^4 + 2x^3 + x^2 + x + 1$ *div* $x^2 + 2x + 1 = x^3 + 2x^2 + 2$.

2. *En* $\mathbb{Z}_5[x]$:

   $x^5 + x^4 + 2x^3 + x^2 + x + 1$ *mód* $x^2 + 2x + 1 = 6x$
   $x^5 + x^4 + 2x^3 + x^2 + x + 1$ *div* $x^2 + 2x + 1 = x^3 + 4x^2 + 3x + 1$.

Definición 43. *Sea* $p(x) \in A[x]$ *y* $a \in A$. *Se dice que* a *es una raíz de* $p(x)$ *si* $p(a) = 0$.

Ejemplo 3.2.4. *El polinomio* $p(x) = x^5 + x^4 + x^3 + 2x^2 + 1 \in \mathbb{Z}_3[x]$ *tiene a* $x = 1$ *por raíz, pues* $p(1) = 1 + 1 + 1 + 2 + 1 = 0$. *Sin embargo,* 0 *no es raíz pues* $p(0) = 1$ *y* 2 *tampoco es raíz pues* $p(2) = 2^5 + 2^4 + 2^3 + 2 \cdot 2^2 + 1 = 2 + 1 + 2 + 2 + 1 = 2$.

El siguiente resultado es un conocido teorema referente a la división por el polinomio $x - a$.

Teorema 3.2.2 (Teorema del resto)**.** *Sea* $p(x) \in A[x]$ *y* $a \in A$. *Entonces el resto de dividir* $p(x)$ *entre* $x - a$ *es el resultado de evaluar* $p(x)$ *en el punto* a. *Dicho de otra forma*

$$p(x) \text{ mód } x - a = p(a)$$

Demostración: Si dividimos $p(x)$ entre $x - a$ nos da un polinomio de grado menor que 1, luego debe ser un polinomio constante. Se tiene entonces que $p(x) = c(x) \cdot (x - a) + r$. Evaluando en a nos queda que $p(a) = c(a) \cdot (a - a) + r$, es decir, $r = p(a)$. ■

Corolario 3.2.1 (Teorema del factor)**.** *Sea* $p(x) \in A[x]$ *y* $a \in A$. *Entonces* a *es raíz de* $p(x)$ *si, y sólo si,* $(x - a) | p(x)$.

En la siguiente proposición veremos una forma rápida de calcular el cociente y el resto de la división de un polinomio entre $x - a$.

Proposición 3.2.2. *Sea* $p(x) \in A[x]$, $a \in A$. *Supongamos que* $p(x) = a_n x^n + \cdots + a_1 x + a_0$ *y que* $p(x) = (b_{n-1}x^{n-1} + \cdots + b_1 x + b_0)(x - a) + r$. *Entonces:*

$b_{n-1} = a_n$

$b_{i-1} = a_i + b_i a$ *para* $i = 0, 1, \cdots, n - 1$

$r = a_0 + b_0 a$

La demostración se deja como ejercicio.

Esta proposición proporciona el conocido método de Ruffini (algoritmo de Horner) para dividir un polinomio entre $x - a$.

Para esto se disponen los datos conocidos como sigue:

	a_n	a_{n-1}	$\cdots$	a_{i+1}	a_i	$\cdots$	a_1	a_0
a								
	b_{n-1}	b_{n-2}	$\cdots$	b_i	b_{i-1}	$\cdots$	b_0	r

Para calcular los coeficientes b_i se procede como sigue:

Se comienza por $b_{n-1} = a_n$

Supuesto calculado b_i se calcula b_{i-1} como $b_{i-1} = a_i + b_i a$.

Por último, hallado b_0 se calcula r como $r = a_0 + b_0 a$.

Para ordenar los cálculos se coloca el valor $b_i a$ justo debajo del valor de a_i, y se efectúa la suma, obteniéndose así el valor de b_{i-1}.

	a_n	a_{n-1}	$\cdots$	a_{i+1}	a_i	$\cdots$	a_1	a_0
a					$b_i a$			
	$b_{n-1} = a_n$	b_{n-2}	$\cdots$	b_i	$b_{i-1} = a_i + b_i a$	$\cdots$	b_0	r

Ejemplo 3.2.5. *Vamos a hallar el cociente y el resto de la división de* $x^5+x^4+x^3+2x^2+1$ *entre* $x-2$ *en* $\mathbb{Q}[x]$. *Para ello procedemos a completar la tabla*

	1	1	1	2	0	1
2						

Rellenando de izquierda a derecha.

	1	1	1	2	0	1
2		$2=1\cdot 2$	$6=3\cdot 2$	$14=7\cdot 2$	$32=16\cdot 2$	$64=32\cdot 2$
	1	$3=1+2$	$7=1+6$	$16=2+14$	$32=0+32$	$65=1+64$

La tabla quedaría así

	1	1	1	2	0	1
2		2	6	14	32	64
	1	3	7	16	32	65

Nótese que $x^5+x^4+x^3+2x^2+1=(x^4+3x^3+7x^2+16x+32)(x-2)+65$, *y que* $p(2)=65$.

Vamos a dividir ahora $x^5+x^4+x^3+2x^2+1$ *entre* $x+1$ *en* $\mathbb{Z}_3[x]$. *Puesto que* $x+1=x-2$, *se tiene que*

	1	1	1	2	0	1
2		2	0	2	2	1
	1	0	1	1	2	2

es decir, el cociente es x^4+x^2+x+2 *y el resto es* 2.

Definición 44. *Sea* $p(x)\in A[x]$, *y* $a\in A$. *Se dice que* a *es una raíz de multiplicidad* m *si* $(x-a)^m|p(x)$ *y* $(x-a)^{m+1}\not| p(x)$.

Nótese que decir que a es una raíz de multiplicidad m es decir que $p(x)=(x-a)^m c(x)$ con $c(a)\neq 0$.

A las raíces de multiplicidad 1 se les llama raíces simples; a las de multiplicidad 2, raíces dobles, a las de multiplicidad 3, raíces triples, y así sucesivamente.

En ocasiones, si a no es una raíz se dice que es una raíz de multiplicidad 0.

Ejemplo 3.2.6. *El polinomio* $x^5+x^3+x^2+1\in\mathbb{Z}_2[x]$ *tiene a* $x=1$ *como raíz triple, pues* $x^5+x^3+x^2+1=(x+1)^3(x^2+x+1)$, *y* x^2+x+1 *no tiene a* 1 *como raíz.*

	1	0	1	1	0	1
1		1	1	0	1	1
	1	1	0	1	1	0
1		1	0	0	1	
	1	0	0	1	0	
1		1	1	1		
	1	1	1	0		
1		1	0			
	1	0	1			

Aquí vemos las sucesivas divisiones por $x+1$. *Se aprecia como las tres primeras son exactas, mientras que la cuarta da resto* 1.

Definición 45. *Sea* K *un cuerpo, y* $p(x),q(x)\in K[x]$. *Se dice que* $d(x)\in K[x]$ *es un máximo común divisor de* $p(x)$ *y* $q(x)$ *si:*

1. $d(x)|p(x)$ *y* $d(x)|q(x)$.
2. *Si* $c(x)|p(x)$ *y* $c(x)|q(x)$ *entonces* $c(x)|d(x)$.

Nota:

1. La primera condición de la definición nos dice que $d(x)$ debe ser un divisor común de $p(x)$ y $q(x)$. La segunda condición nos dice que este divisor común es el "más grande" de los divisores comunes.
2. Si $d(x)$ es un máximo común divisor de $p(x)$ y $q(x)$ y $a \in K^*$ entonces $a \cdot d(x)$ es también un máximo común divisor de $p(x)$ y $q(x)$. De hecho, cualquier polinomio que sea un máximo común divisor de $p(x)$ y $q(x)$ es de la forma $a \cdot d(x)$. De todos estos, hay uno, y sólo uno que es mónico (salvo en el caso de que $p(x) = q(x) = 0$). Denotaremos por $mcd(p(x), q(x))$ al único máximo común divisor de $p(x)$ y $q(x)$ que es mónico.
3. La definición anterior podría haberse hecho tomando coeficientes en un anillo. En el caso de $A = \mathbb{Z}$, si $d(x)$ es un máximo común divisor de $p(x)$ y $q(x)$, también lo es $-d(x)$, y no hay más. Denotaremos por $mcd(p(x), q(x))$ al que tenga coeficiente líder positivo.
4. Aquí se ha definido el máximo común divisor de dos polinomios. Podría haberse definido de forma análoga el máximo común divisor de 3 ó más.

Se deja como ejercicio dar la definición de mínimo común múltiplo.

Veremos a continuación algunas propiedades referentes al máximo común divisor. Supongamos que tenemos $p(x), q(x), r(x), d(x) \in K[x]$, y supondremos que los cuatro polinomios son mónicos.

Propiedades:

1. $mcd(p(x), q(x)) = mcd(a \cdot p(x), q(x)) = mcd(p(x), a \cdot q(x))$, donde $a \in K^*$.
2. $mcd(p(x), 0) = p(x)$ y $mcd(p(x), 1) = 1$
3. Si $p(x)|q(x)$ entonces $mcd(p(x), q(x)) = p(x)$.
4. $mcd(p(x), mcd(q(x), r(x)) = mcd(mcd(p(x), q(x)), r(x)) = mcd(p(x), q(x), r(x))$.
5. $mcd(p(x) \cdot r(x), q(x) \cdot r(x)) = mcd(p(x), q(x)) \cdot r(x)$
6. Si $d(x)|p(x)$ y $d(x)|q(x)$ entonces $mcd\left(\frac{p(x)}{d(x)}, \frac{q(x)}{d(x)}\right) = \frac{mcd(p(x),q(x))}{d(x)}$.

Como ejercicio, se deja enunciar propiedades análogas para el mínimo común múltiplo, así como para polinomios en $\mathbb{Z}[x]$.

Los siguientes resultados son análogos a los dados para números enteros.

Lema 3.2.1. *Sean* $p(x), q(x) \in K[x]$. *Entonces, para cualquier* $c(x) \in K[x]$ *se tiene que* $mcd(p(x), q(x)) = mcd(q(x), p(x) - c(x)q(x))$.

Corolario 3.2.2. *Sean* $p(x), q(x) \in K[x]$, *con* $q(x) \neq 0$. *Entonces* $mcd(p(x), q(x)) = mcd(q(x), p(x)$ *mód* $q(x))$.

Para calcular ahora el máximo común divisor de dos polinomios procedemos de igual forma que a la hora de calcular el máximo común divisor de dos números enteros. Vamos realizando divisiones hasta obtener un resto nulo. El resto anterior es el máximo común divisor.

$$\begin{aligned}
p(x) &= q(x)\cdot c_1(x) + r_1(x)\\
q(x) &= r_1(x)\cdot c_2(x) + r_2(x)\\
r_1(x) &= r_2(x)\cdot c_3(x) + r_3(x)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
r_{i-2}(x) &= r_{i-1}(x)\cdot c_i(x) + r_i(x)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
r_{k-2}(x) &= r_{k-1}(x)\cdot c_k(x) + r_k(x)\\
r_{k-1}(x) &= r_k(x)\cdot c_{k+1}(x) + 0
\end{aligned}$$

Sin embargo, el polinomio $r_k(x)$ no tiene por qué ser mónico, luego el resultado final, $r_k(x)$, no sería el máximo común divisor de $p(x)$ y $q(x)$. Necesitamos multiplicar por el inverso del coeficiente líder para obtener el máximo común divisor.

El algoritmo EUCLIDES del capítulo anterior vale ahora para el cálculo del máximo común divisor de dos polinomios con coeficientes en un cuerpo. Únicamente, al final hay que multiplicar el resultado por el inverso del coeficiente líder de $p(x)$.

En el caso de que los dos polinomios, $p(x)$ y $q(x)$ fueran nulos, el algoritmo daría error.

Algoritmo EUCLIDES$(p(x), q(x))$

Entrada: $p(x), q(x) \in K[x]$

Salida: $d(x) = mcd(p(x), q(x))$

Mientras $q(x) \neq 0$

$(p(x), q(x)) := (q(x), p(x) \text{ mód } q(x))$

$a = c.l.(p(x))^{-1}$.

$p(x) := a \cdot p(x)$.

Devuelve $p(x)$

Ejemplo 3.2.7. *Vamos a calcular en $\mathbb{Q}[x]$ el máximo común divisor de $x^3 - x + 3$ y $x^3 + x^2 + 1$.*

$$\begin{array}{rcrlcr}
x^3 - x + 3 &=& (x^3 + x^2 + 1) & 1 & + & (-x^2 - x + 2)\\
x^3 + x^2 + 1 &=& (-x^2 - x + 2) & (-x) & + & 2x + 1\\
-x^2 - x + 2 &=& (2x + 1) & \left(\frac{-1}{2}x - \frac{1}{4}\right) & + & \frac{9}{4}\\
2x + 1 &=& \frac{9}{4} & \left(\frac{8}{9}x + \frac{4}{9}\right) & + & 0
\end{array}$$

Luego un máximo común divisor de $x^3 - x + 3$ y $x^3 + x^2 + 1$ es $\frac{9}{4}$. Multiplicamos por $\frac{4}{9}$ y obtenemos que $mcd(x^3 - x + 3, x^3 + x^2 + 1) = 1$.

$p(x)$	$q(x)$	a
$x^3 - x + 3$	$x^3 + x^2 + 1$	
$x^3 + x^2 + 1$	$-x^2 - x + 2$	
$-x^2 - x + 2$	$2x + 1$	
$2x + 1$	$\frac{9}{4}$	
$\frac{9}{4}$	0	$\frac{4}{9}$
1		

El teorema de Bezout se tiene también en el caso de los polinomios.

Teorema 3.2.3. *Sean $p(x), q(x) \in K[x]$, y sea $d(x) = mcd(p(x), q(x))$. Entonces existen $u(x), v(x) \in K[x]$ tales que $d(x) = p(x)\cdot u(x) + q(x)\cdot v(x)$*

La demostración del teorema, así como el algoritmo para calcular $u(x)$ y $v(x)$ es análogo al hecho en el caso de los números enteros. Hay que tener en cuenta que al final, hay que multiplicar el resultado por el inverso del coeficiente líder.

Algoritmo BEZOUT$(p(x), q(x))$
Entrada: $p(x), q(x) \in K[x]$
Salida: $(d(x), u(x), v(x))$: $d(x) = mcd(p(x), q(x));\ d(x) = p(x) \cdot u(x) + q(x) \cdot v(x)$
  Si $q(x) = 0$
    $a := c.l.(p(x))^{-1}$
    Devuelve $(a \cdot p(x), a, 0)$;
    Fin
  $r_{-1}(x) := p(x)$, $r_0(x) := q(x)$.
  $u_{-1}(x) := 1$, $u_0(x) := 0$.
  $v_{-1}(x) := 0$, $v_0(x) := 1$.
  $i := 1$.
  $r_1(x) := r_{-1}(x)$ mód $r_0(x)$
  Mientras $r_i(x) \neq 0$
    $c_i(x) := r_{i-2}(x)$ div $r_{i-1}(x)$.
    $u_i(x) := u_{i-2}(x) - u_{i-1}(x) \cdot c_i(x)$.
    $v_i(x) := v_{i-2}(x) - v_{i-1}(x) \cdot c_i(x)$.
    $i := i + 1$.
    $r_i(x) := r_{i-2}(x)$ mód $r_{i-1}(x)$.
  $a := c.l.(r_{i-1}(x))^{-1}$
  $r(x) := a \cdot r_{i-1}(x)$; $u(x) := a \cdot u_{i-1}(x)$; $v(x) := a \cdot v_{i-1}(x)$.
  Devuelve $(r(x), u(x), v(x))$.
  Fin

Ejemplo 3.2.8.

1. *Vamos a expresar* $mcd(x^3 - x + 3, x^3 + x^2 + 1)$ *en función de los polinomios* $x^3 - x + 3$ *y* $x^3 + x^2 + 1$.

i	a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
-1		$x^3 - x + 3$		1	0
0		$x^3 + x^2 + 1$		0	1
1		$-x^2 - x + 2$	1	1	-1
2		$2x - 1$	$-x$	x	$-x + 1$
3		$\frac{9}{4}$	$\frac{-1}{2}x - \frac{1}{4}$	$\frac{1}{2}x^2 + \frac{1}{4}x + 1$	$\frac{-1}{2}x^2 + \frac{1}{4}x - \frac{3}{4}$
4	$\frac{4}{9}$	0			
		$\mathbf{1}$		$\mathbf{\frac{2}{9}x^2 + \frac{1}{9}x + \frac{4}{9}}$	$\mathbf{\frac{-2}{9}x^2 + \frac{1}{9}x - \frac{3}{9}}$

Aquí vemos cómo se han obtenido las dos últimas columnas:

$$1 = 1 - 1 \cdot 0 \qquad -1 = 0 - 1 \cdot 1$$
$$x = 0 - (-x) \cdot 1 \qquad -x + 1 = 1 - (-x) \cdot (-1)$$
$$\tfrac{1}{2}x^2 + \tfrac{1}{4}x + 1 = 1 - \left(\tfrac{-1}{2}x - \tfrac{1}{4}\right) \cdot x \qquad \tfrac{-1}{2}x^2 + \tfrac{1}{4}x - \tfrac{3}{4} = -1 - \left(\tfrac{-1}{2}x - \tfrac{1}{4}\right) \cdot (-x + 1)$$

Nótese que se verifica que

$$1 = (x^3 - x + 3)\left(\frac{2}{9}x^2 + \frac{1}{9}x + \frac{4}{9}\right) + (x^3 + x^2 + 1)\left(\frac{-2}{9}x^2 + \frac{1}{9}x - \frac{3}{9}\right)$$

2. *Sean* $p(x) = x^5 + 2x^4 + x^2 + 2x + 2$, $q(x) = x^5 + 2x^3 + x^2 + x + 1 \in \mathbb{Z}_3[x]$. *Vamos a calcular su máximo común divisor y a exprearlo en función de* $p(x)$ *y* $q(x)$.

i	a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
-1		$x^5 + 2x^4 + x^2 + 2x + 2$		1	0
0		$x^5 + 2x^3 + x^2 + x + 1$		0	1
1		$2x^4 + x^3 + x + 1$	1	1	2
2		$2x^2 + 2$	$2x + 2$	$x + 1$	$2x$
3	2	0			
		$\mathbf{x^2 + 1}$		$\mathbf{2x + 2}$	$\mathbf{x}$

Luego $mcd(x^5 + 2x^4 + x^2 + 2x + 2, x^5 + 2x^3 + x^2 + x + 1) = x^2 + 1$ *y*

$$x^2 + 1 = (x^5 + 2x^4 + x^2 + 2x + 2)(2x + 2) + (x^5 + 2x^3 + x^2 + x + 1)(x)$$

3. *En* $\mathbb{Z}[x]$ *se tiene que* $mcd(x, 2) = 1$. *Sin embargo no es posible encontrar* $u(x), v(x) \in \mathbb{Z}[x]$ *tales que* $x \cdot u(x) + 2 \cdot v(x) = 1$.

Los Corolarios 2.3.2, 2.3.3 y 2.3.4, así como la Proposición 2.3.1 pueden ahora trasladarse al contexto de polinomios con coeficientes en un cuerpo.

También las Proposiciones 2.4.1 y 2.4.2 son válidas para polinomios.

Más precisamente, sean $a(x), b(x), c(x) \in K[x]$. Entonces la ecuación $a(x)u(x) + b(x)v(x) = c(x)$ tiene solución si, y sólo si, $mcd(a(x), b(x))|c(x)$.

Si $u_0(x)$, $v_0(x)$ es una tal solución, y $d(x) = mcd(a(x), b(x))$, entonces todas las soluciones son de la forma:

$$\begin{array}{l} u(x) = u_0(x) + p(x)\frac{b(x)}{d(x)} \\ v(x) = v_0(x) - p(x)\frac{a(x)}{d(x)} \end{array} \qquad p(x) \in K[x]$$

Ejemplo 3.2.9. *Vamos a hallar todas las parejas de polinomio* $u(x), v(x) \in \mathbb{Z}_3[x]$ *que satisfacen la ecuación*

$$(x^5 + 2x^3 + 2) \cdot u(x) + (x^5 + 2x^4 + 2x^3 + 1) \cdot v(x) = x^4 + 2x^2 + 2x + 2$$

Para esto, vemos en primer lugar si existe alguno. Esto ocurre si, y sólo si, $x^4 + 2x^2 + 2x + 2$ *es múltiplo de* $mcd(x^5 + 2x^3 + 2, x^5 + 2x^4 + 2x^3 + 1)$.

a	$a(x)$	$b(x)$	$c(x)$
	$x^5 + 2x^3 + 2$	$x^5 + 2x^4 + 2x^3 + 1$	1
	$x^5 + 2x^4 + 2x^3 + 1$	$x^4 + 1$	$x + 2$
	$x^4 + 1$	$2x^3 + 2x + 2$	$2x$
	$2x^3 + 2x + 2$	$2x^2 + 2x + 1$	
2	$2x^2 + 2x + 1$	0	
	$x^2 + x + 2$		

luego $mcd(x^5+2x^3+2, x^5+2x^4+2x^3+1) = x^2+x+2$, *y como* $x^4+2x^2+2x+2 = (x^2+x+2)(x^2+2x+1)$, *es decir,* $(x^2 + x + 2)|(x^4 + 2x^2 + 2x + 2)$ *sabemos que podemos encontrar parejas de polinomio* $u(x), v(x)$ *que sean solución de la ecuación anterior.*

Buscamos dos polinomios $u_0(x)$, $v_0(x)$ *que sean solución. Para eso, completamos la tabla anterior.*

a	$r(x)$	$c(x)$	$u(x)$	$v(x)$
	x^5+2x^3+2		1	0
	$x^5+2x^4+2x^3+1$		0	1
	x^4+1	1	1	2
	$2x^3+2x+2$	$x+2$	$2x+1$	x
	$2x^2+2x+1$	$2x$	$2x^2+x+1$	x^2+2
2	0			
	$\mathbf{x^2+x+2}$		$\mathbf{x^2+2x+2}$	$\mathbf{2x^2+1}$

Tomamos entonces

$$\begin{array}{rcrcl} u_0(x) & = & (x^2+2x+2)\cdot(x^2+2x+1) & = & x^4+x^3+x^2+2 \\ v_0(x) & = & (2x^2+1)\cdot(x^2+2x+1) & = & 2x^4+x^3+2x+1 \end{array}$$

Puesto que
$(x^5+2x^3+2)\ div\ (x^2+x+2) = x^3+2x^2+x+2$
$(x^5+2x^4+2x^3+1)\ div\ (x^2+x+2) = x^3+x^2+2x+2$
tenemos que la solución general es

$$\begin{array}{rcrcrl} u(x) & = & x^4+x^3+x^2+2 & + & (x^3+x^2+2x+2)\cdot p(x) & \\ v(x) & = & 2x^4+x^3+2x+1 & + & 2(x^3+2x^2+x+2)\cdot p(x) & p(x)\in\mathbb{Z}_3[x] \end{array}$$

3.3. Factorización de polinomios

En esta sección veremos como los polinomios con coeficientes en un cuerpo se pueden factorizar como producto de irreducibles.

3.3.1. Polinomios irreducibles.

Comenzamos con la definición de polinomios irreducibles.

Definición 46. *Sea $p(x)\in K[x]$ no constante. Se dice que $p(x)$ es irreducible si sus únicos divisores son los polinomios constantes (no nulos) y los polinomios de la forma $a\cdot p(x) : a\in K^*$.*

Sea $p(x)\in\mathbb{Z}[x]$, $p(x)\neq 0,1,-1$. Se dice que $p(x)$ es irreducible si sus únicos divisores son ± 1 y $\pm p(x)$.

Si $p(x)$ no es irreducible, se dice que es reducible.

Observación: Nótese que si $p(x)\in K[x]$ es reducible y $gr(p(x))=n$ entonces $p(x)$ tiene un divisor no constante de grado menor o igual que $\frac{n}{2}$.

Ejemplo 3.3.1.

1. *Cualquier polinomio de grado 1 en $K[x]$ es irreducible. Sin embargo, el polinomio $p(x)=2x+2$ es reducible en $\mathbb{Z}[x]$, pues $2|p(x)$ y $x+1|p(x)$.*

2. *El polinomio $x^3+x+1\in\mathbb{Z}_2[x]$ es irreducible. Por la observación anterior debe tener un divisor de grado menor o igual que $\frac{3}{2}$. Los únicos polinomios en esas condiciones son x y $x+1$, y ninguno de ellos divide a x^3+x+1.*

3. *Dado $p(x)=ax^2+bx+c\in\mathbb{R}[x]$ entonces $p(x)$ es irreducible si, y sólo si, $b^2-4ac<0$.*

Al igual que en el caso de $\mathbb{Z}$ se tiene ahora:

Proposición 3.3.1. *Sea $p(x) \in K[x]$ no constante. Entonces:*

$$p(x) \text{ es irreducible } \iff \big(p(x)|q_1(x)\cdot q_2(x) \Longrightarrow p(x)|q_1(x) \text{ ó } p(x)|q_2(x)\big)$$

Con esta proposición estamos ya en condiciones de dar el teorema de factorización.

Teorema 3.3.1. *Sea K un cuerpo, y $p(x) \in K[x]$ no constante. Entonces $p(x)$ se expresa de forma única como*

$$p(x) = ap_1(x)p_2(x)\cdots p_k(x)$$

donde $a \in K$ y $p_i(x)$ es un polinomio mónico e irreducible.

La demostración es similar a la que se hizo del teorema fundamental de la aritmética.

En $\mathbb{Z}_8[x]$ se tiene que $x^2+7 = (x+1)(x+7) = (x+3)(x+5)$. Vemos entonces que podemos factorizar un polinomio de dos formas distintas. Sin embargo, puesto que $\mathbb{Z}_8$ no es un cuerpo, este ejemplo no está en contradicción con la afirmación de la factorización única que nos da el teorema 3.3.1.

En el caso de polinomios con coeficientes en $\mathbb{Z}$ la situación es algo diferente, pues en general no es posible expresar un polinomio irreducible como una constante por un polinomio mónico. Por ejemplo, $2x^2+4x+1$ es irreducible. Si lo expresamos como una constante por un polinomio mónico nos queda $2\left(x^2+2x+\frac{1}{2}\right)$ que no pertenece a $\mathbb{Z}[x]$. El papel de polinomio mónico lo juega aquí lo que se llama polinomio primitivo.

Definición 47. *Sea $p(x) \in \mathbb{Z}[x]$ no nulo. Se llama* contenido *de $p(x)$ al máximo común divisor de sus coeficientes. Es decir, si $p(x) = a_nx^n + \cdots + a_1x + a_0$, entonces*

$$c(p(x)) = mcd(a_0, a_1, \cdots, a_n)$$

Un polinomio se dice primitivo *si su contenido vale 1.*

Obviamente, dado $p(x) \in \mathbb{Z}[x]$, entonces $p(x)$ se expresa como $p(x) = c(p(x))\cdot p_1(x)$, donde $p_1(x)$ es un polinomio primitivo. Más en general, si $p(x) \in \mathbb{Q}[x]$, existe $\frac{a}{b} \in \mathbb{Q}$ y $p_1(x) \in \mathbb{Z}[x]$ primitivo tal que $p(x) = \frac{a}{b}p_1(x)$.

Ejemplo 3.3.2. *El contenido del polinomio $6x^3+9x^2-15x+12$ es 3, pues $mcd(6,9,-15,12) = 3$. Se tiene entonces que $p(x) = 3\cdot(2x^3+3x^2-5x+4)$. Fácilmente se comprueba que $2x^3+3x^2-5x+4$ es primitivo.*

Consideramos el polinomio $p(x) = 7x^3 - \frac{7}{5}x^2 + \frac{14}{3}x - \frac{7}{3} \in \mathbb{Q}[x]$. Multiplicamos por el mínimo común múltiplo de los denominadores, que es 15, y nos queda:

$$p(x) = \frac{1}{15}(105x^3 - 21x^2 + 70x - 35)$$

y como este último polinomio tiene contenido igual a 7 resulta que

$$p(x) = \frac{7}{15}(15x^3 - 3x^2 + 10x - 5)$$

El teorema de factorización de polinomios en $\mathbb{Z}[x]$ dice:

Teorema 3.3.2. *Sea $q(x) \in \mathbb{Z}[x]$, $q(x) \neq 0, 1, -1$. Entonces $q(x)$ se factoriza como*

$$q(x) = p_1\cdots p_rq_1(x)\cdots q_s(x)$$

donde p_i son números enteros primos y $q_j(x)$ son polinomios primitivos irreducibles en $\mathbb{Q}[x]$.

Más adelante estudiaremos esto con un poco más de detalle.

3.3.2. Raíces de polinomios.

Sabemos que si tenemos $p(x) \in K[x]$, entonces $p(x)$ se expresa de forma única como producto de irreducibles. Sin embargo, en general no es fácil encontrar estos irreducibles. Existen resultados que permiten encontrar esta factorización cuando $K = \mathbb{Z}_p$ (algoritmo de Berlekamp), o $K = \mathbb{Q}$ (método de Kronecker o lema de Hensel) que se escapan de los objetivos de estas notas. Nosotros vamos a estudiar los métodos más sencillos.

A la hora de encontrar de encontrar los divisores irreducibles de un polinomio vamos a comenzar por los más simples: los de grado 1. Por tanto, vamos a buscar divisores de la forma $x - a$ con $a \in K$. Por el teorema 3.2.1 sabemos que encontrar un divisor de la forma $x - a$ es equivalente a encontrar una raíz $x = a$. En este apartado nos vamos a dedicar a ver cómo encontrar las raíces de polinomios.

Vamos a distinguir según el cuerpo en el que estemos trabajando.

Raíces de polinomios con coeficientes complejos.

Comenzamos con en el caso $K = \mathbb{C}$. El teorema fundamental del álgebra nos dice que todo polinomio no constante con coeficientes complejos tiene al menos una raíz.

Si $p(x) \in \mathbb{C}[x]$ y a_1 es una raíz, entonces $p(x) = (x - a_1) \cdot p_1(x)$. Si ahora le volvemos a aplicar el mismo resultado a $p_1(x)$ tendremos $p(x) = (x - a_1) \cdot (x - a_2) \cdot p_2(x)$ (donde a_2 podría ser igual a a_1). Repitiendo el proceso, tenemos que $p(x) = a \cdot (x - a_1) \cdot (x - a_2) \cdots (x - a_n)$. Es decir, todo polinomio de grado n con coeficientes complejos se descompone como producto de n irreducibles de grado 1 (algunos podrían aparecer repetidos).

Por ejemplo, el polinomio $p(x) = x^3 - 2x^2 + x - 2$ tiene a $x = i$ como raíz. Si dividimos por $x - i$ nos queda $p(x) = (x - i) \cdot (x^2 + (-2 + i)x - 2i)$. Este tiene a $x = -i$ como raíz. Volviendo a dividir tenemos $p(x) = (x - i) \cdot (x + i) \cdot (x - 2)$.

El problema es que no tenemos forma de determinar las raíces complejas de un polinomio salvo algunos casos muy concretos.

Raíces de polinomios con coeficientes reales.

Si $p(x)$ es un polinomio con coeficientes reales de grado impar, sabemos, por el teorema de Bolzano, que tiene al menos una raíz real (pues los límites de la función $p(x)$ en $+\infty$ y $-\infty$ tienen signo distinto).

Por ejemplo, si $p(x) = x^3 - 7x^2 + 5x - 3$, entonces el límite cuando $x \to +\infty$ es $+\infty$ mientras que el límite cuando $x \to -\infty$ es $-\infty$. Luego debe haber algún punto en el que $p(x)$ valga cero. De hecho, $p(6) = -9$ y $p(7) = 32$, luego $p(x)$ tiene una raíz en el intervalo $]6, 7[$.

Pero al igual que antes, no tenemos forma de calcular esa raíz (bueno, podríamos aproximarla utilizando algún método numérico para tal efecto).

Para polinomios de grado 2, podemos encontrar las raíces con la conocida expresión $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Por ejemplo, el polinomio $x^2 - x - 1$ tiene como raíces a $x_1 = \frac{1+\sqrt{5}}{2}$ (número áureo) y $x_2 = \frac{1-\sqrt{5}}{2}$. Por tanto, tenemos que

$$x^2 - x - 1 = \left(x - \frac{1 + \sqrt{5}}{2}\right) \cdot \left(x - \frac{1 - \sqrt{5}}{2}\right)$$

> Cuando decimos que una raíz es $\frac{1+\sqrt{5}}{2}$ tampoco hemos calculado una raíz del polinomio. Simplemente hemos puesto una raíz del polinomio $x^2 - x - 1$ en función de una raíz del polinomio $x^2 - 5$, y a esta raíz le hemos puesto un nombre ($\sqrt{5}$). Pero lo único que podemos conseguir es una aproximación de ese número con tanta precisión como queramos, al igual que cuando hablábamos de una raíz de $x^3 - 7x^2 + 5x - 3$.

Si tenemos ahora un polinomio $p(x) \in \mathbb{R}[x]$ que no tiene raíces reales, sabemos que tiene al menos una raíz compleja $\alpha = a + bi$. En tal caso, $\overline{\alpha} = a - bi$ es también una raíz de $p(x)$, y $(x - \alpha) \cdot (x - \overline{\alpha})$ es un divisor de $p(x)$. Como ese producto tiene los coeficientes reales (pues vale $(x - a)^2 + b^2$), podemos asegurar que $p(x)$ tiene un divisor de grado 2.

Deducimos entonces que todo polinomio irreducible real, o es de grado uno, o es de grado 2 y no tiene raíces reales.

Ejemplo 3.3.3.

1. *Sea $p(x) = x^3 - 1$. Es claro que $x = 1$ es una raíz de este polinomio. Sus raíces complejas son las tres raíces de la unidad, que son*

$cos(0)+i\ sen(0)=1;\quad \omega=cos(\frac{2\pi}{3})+i\ sen(\frac{2\pi}{3})=\frac{-1}{2}+i\frac{\sqrt{3}}{2};\quad \overline{\omega}=\omega^2=cos(\frac{4\pi}{3})+i\ sen(\frac{4\pi}{3})=\frac{-1}{2}-i\frac{\sqrt{3}}{2}$

Por tanto, su factorización en $\mathbb{C}[x]$ *es* $p(x)=(x-1)(x-\omega)(x-\overline{\omega})$.

El producto $(x-\omega)(x-\overline{\omega})$ *vale* x^2+x+1, *que tiene los coeficientes reales. Por tanto, la factorización de* $p(x)$ *en* $\mathbb{R}[x]$ *es* $p(x)=(x-1)(x^2+x+1)$.

2. *Sea ahora* $p(x)=x^8-1$. *Este polinomio tiene 8 raíces complejas, que son:*

$$\begin{array}{ll}\alpha_0=cos(0)+i\ sen(0)=1 & \alpha_1=cos(\frac{2\pi}{8})+i\ sen(\frac{2\pi}{8})=\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\\ \alpha_2=(\alpha_1)^2=cos(\frac{4\pi}{8})+i\ sen(\frac{4\pi}{8})=i & \alpha_3=(\alpha_1)^3=cos(\frac{6\pi}{8})+i\ sen(\frac{6\pi}{8})=\frac{-\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\\ \alpha_4=(\alpha_1)^4=cos(\frac{8\pi}{8})+i\ sen(\frac{8\pi}{8})=-1 & \alpha_5=(\alpha_1)^5=cos(\frac{10\pi}{8})+i\ sen(\frac{10\pi}{8})=\frac{-\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\\ \alpha_6=(\alpha_1)^6=cos(\frac{12\pi}{8})+i\ sen(\frac{12\pi}{8})=-i & \alpha_7=(\alpha_1)^7=cos(\frac{14\pi}{8})+i\ sen(\frac{14\pi}{8})=\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\end{array}$$

Notemos como $\overline{\alpha_1}=\alpha_7$, $\overline{\alpha_2}=\alpha_6$ *y* $\overline{\alpha_3}=\alpha_5$.

La factorización de $p(x)$ *en* $\mathbb{C}[x]$ *sería* $\prod_{i=0}^{7}(x-\alpha_i)$.

Podemos ver como $(x-\alpha_1)(x-\alpha_7)=x^2-\sqrt{2}x+1$, $(x-\alpha_2)(x-\alpha_6)=(x-i)(x+i)=x^2+1$ *y* $(x-\alpha_3)(x-\alpha_5)=x^2+\sqrt{2}x+1$. *La factorización de* $p(x)$ *en* $\mathbb{R}[x]$ *es entonces*

$$p(x)=(x-1)(x+1)(x^2+1)(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$$

Y por último, puesto que $(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)=x^4+1$, *la factorización de* $p(x)$ *en* $\mathbb{Q}[x]$ *es*

$$p(x)=(x-1)(x+1)(x^2+1)(x^4+1)$$

Raíces de polinomios con coeficientes en $\mathbb{Z}_p$.

En este caso, y puesto que el número de elementos de $\mathbb{Z}_p$ es finito, la forma que tenemos de buscar las raíces es probando con los distintos elementos de $\mathbb{Z}_p$.

Por tanto, si $q(x)\in\mathbb{Z}_p[x]$, para ver si tiene raíces, lo que tenemos que hacer es evaluar el polinomio en los distintos elementos de $\mathbb{Z}_p$. Es decir, calculamos $q(0),\ q(1),\cdots q(p-1)$, y comprobamos si en algún caso nos ha dado cero.

Ejemplo 3.3.4. 1. *Sea* $p(x)=x^3+x+1\in\mathbb{Z}_2[x]$. *Entonces* $p(0)=1$ *y* $p(1)=1$. *Como* $\mathbb{Z}_2=\{0,1\}$, *el polinomio* $p(x)$ *no tiene raíces.*

2. *Sea ahora* $p(x)=x^3+x+1\in\mathbb{Z}_3[x]$. *Ahora se tiene que* $p(1)=0$, *luego* $x=1$ *es una raíz. Probamos a dividir por* $x-1$.

	1	0	1	1
1		1	1	2
	1	1	2	0

Luego $p(x)=(x+2)\cdot(x^2+x+2)$. *Puede comprobarse fácilmente que* x^2+x+2 *no tiene raíces.*

3. *Sea* $p(x)=x^4+3x^3+2x^2+6x+5\in\mathbb{Z}_7[x]$. *Vamos a encontrar sus raíces. Para eso, vamos a ir probando por los distintos elementos de* $\mathbb{Z}_7$. *Claramente,* $p(0)=5\neq 0$.

	1	3	2	6	5
1		1	4	6	5
	1	4	6	5	3

	1	3	2	6	5
2		2	3	3	4
	1	5	5	2	2

	1	3	2	6	5
3		3	4	4	2
	1	6	6	3	0

Luego $x = 3$ es una raíz, y $p(x) = (x-3)\cdot(x^3+6x^2+6x+3)$. Ahora seguimos buscando raíces, pero lo hacemos con el polinomio x^3+6x^2+6x+3. Con $x = 0$, $x = 1$ y $x = 2$ ya no tenemos que probar, pues lo hemos hecho antes.

$$\begin{array}{c|cccc} & 1 & 6 & 6 & 3 \\ 3 & & 3 & 6 & 1 \\ \hline & 1 & 2 & 5 & 4 \end{array} \qquad \begin{array}{c|cccc} & 1 & 6 & 6 & 3 \\ 4 & & 4 & 5 & 2 \\ \hline & 1 & 3 & 4 & 5 \end{array} \qquad \begin{array}{c|cccc} & 1 & 6 & 6 & 3 \\ 5 & & 5 & 6 & 4 \\ \hline & 1 & 4 & 5 & 0 \end{array}$$

Y vemos que $x = 5$ es otra raíz. Tenemos entonces que $p(x) = (x-3)\cdot(x-5)\cdot(x^2+4x+5)$. Continuamos ahora con x^2+4x+5.

$$\begin{array}{c|ccc} & 1 & 4 & 5 \\ 5 & & 5 & 3 \\ \hline & 1 & 2 & 1 \end{array} \qquad \begin{array}{c|ccc} & 1 & 4 & 5 \\ 6 & & 6 & 4 \\ \hline & 1 & 3 & 2 \end{array}$$

Y por tanto, $p(x)$ no tiene más raíces. Tendríamos entonces la siguiente factorización del polinomio $p(x)$:

$$p(x) = (x+4)\cdot(x+2)\cdot(x^2+4x+5).$$

Raíces de polinomios con coeficientes en $\mathbb{Q}$.

Vamos a terminar este apartado viendo cómo encontrar las raíces racionales de un polinomio con coefientes en $\mathbb{Q}$.

Notemos en primer lugar que si $p(x) \in \mathbb{Q}[x]$, entonces podemos multiplicar $p(x)$ por una constante r de forma que el polinomio $r\cdot p(x)$ tenga los coeficientes enteros y sea primitivo (ver definición 47). Y las raíces de $p(x)$ y $r\cdot p(x)$ son las mismas.

Por tanto, tomamos $p(x) \in \mathbb{Z}[x]$ primitivo, y nos proponemos calcular sus raíces racionales.

Tenemos el siguiente resultado.

Proposición 3.3.2. *Sea $q(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio con coeficientes en $\mathbb{Z}$ y primitivo, y sea $\frac{a}{b} \in \mathbb{Q}$. Supongamos que $mcd(a,b) = 1$. Entonces, si $\frac{a}{b}$ es una raíz de $q(x)$, se verifica que $a|a_0$ y $b|a_n$.*

Demostración: Por ser $\frac{a}{b}$ una raíz de $q(x)$ se tiene que $q\left(\frac{a}{b}\right) = 0$, es decir,

$$a_n\left(\frac{a}{b}\right)^n + \cdots + a_1\frac{a}{b} + a_0 = 0 \Longrightarrow a_n a^n + a_{n-1}a^{n-1}b + \cdots + a_1 a b^{n-1} + a_0 b^n = 0,$$

y de aquí se tiene, por una parte que

$$a_0 b^n = -a(a_n a^{n-1} + a_{n-1}a^{n-2}b + \cdots a_1 b^{n-1},$$

lo que implica que $a|(a_0 b^n)$, y por tanto $a|a_0$ (ya que $mcd(a,b) = 1$. Ver corolario 2.3.4); y por otra parte que

$$a_n a^n = -b(a_{n-1}a^{n-1} + \cdots + a_1 a b^{n-2} + a_0 b^{n-1},$$

lo que implica que $b|a_n$. ■

Ejemplo 3.3.5. *Consideramos el polinomio $q(x) = 2x^3+3x^2-5x+1$. Sus posibles raíces racionales son ± 1 y $\pm\frac{1}{2}$, pues el numerador tiene que ser un divisor de 1 y el denominador un divisor de 2. Evaluamos en esos puntos y obtenemos:*

$$q(1) = 1 \qquad q(-1) = 7 \qquad q\left(\frac{1}{2}\right) = \frac{-1}{2} \qquad q\left(\frac{-1}{2}\right) = 4$$

luego $q(x)$ no tiene raíces racionales.

Aunque esta proposición nos acota bastante el número de posibles raíces, haciendo uso únicamente de la proposición éste podría ser bastante elevado.

Ejemplo 3.3.6. *Sea* $q(x) = 6x^4 + 11x^3 - 19x^2 + 18x - 8$. *Si nos atenemos a la proposición 3.3.3 las posibles raíces de* $q(x)$ *son*

Con denominador 1*:* $1, 2, 4, 8, -1, -2, -4, -8$.
Con denominador 2*:* $\frac{1}{2}, \frac{-1}{2}$ *(pues las otras ya las hemos considerado).*
Con denominador 3*:* $\frac{1}{3}, \frac{2}{3}, \frac{4}{3}, \frac{8}{3}, \frac{-1}{3}, \frac{-2}{3}, \frac{-4}{3}, \frac{-8}{3}$.
Con denominador 6*:* $\frac{1}{6}, \frac{-1}{6}$.
Y vemos que hay un total de 20 *posibles raíces por las que hay probar.*

El siguiente resultado nos permite reducir aún más las posibles raíces de un polinomio con coeficientes en $\mathbb{Z}$.

Proposición 3.3.3. *Sea* $q(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. *Supongamos que* $\frac{a}{b}$ *es una raíz de* $q(x)$, *con* $mcd(a, b) = 1$. *Entonces, para cualquier* $c \in \mathbb{Z}$ *se verifica que* $(bc - a)|p(c)$.

La demostración de esta proposición se hará más adelante.

Si en la proposición anterior tomamos $c = 0$ obtenemos que $a|a_0$.
Si tomamos $c = 1$ obtenemos que $(b - a)|p(1)$.
Si tomamos $c = -1$ obtenemos que $(b + a)|p(-1)$.

Ejemplo 3.3.7. *Retomamos el polinomio* $q(x) = 6x^4 + 11x^3 - 19x^2 + 18x - 8$ *del ejemplo anterior. Entonces* $q(1) = 8$ *y* $q(-1) = -50$.

Tenemos entonces que si $\frac{a}{b}$ *es una raíz de* $q(x)$ *entonces* $b - a$ *es un divisor de* 8. *Podemos entonces eliminar de la lista de posibles raíces las siguientes:* 1 *(esta pues ya hemos calculado* $q(1)$, *y nos ha dado distinto de cero),* 4 *(4 es una fracción con numerador 4 y denominador 1, y la diferencia de ambos es 3, que no es divisor de 8),* 8 *(aquí tenemos que* $b - a = -7$*),* $-2, -4, -8, \frac{-1}{2}, \frac{-2}{3}, \frac{-4}{3}, \frac{8}{3}, \frac{-8}{3}, \frac{1}{6}, \frac{-1}{6}$.

Nos quedan entonces:

$$2 \qquad -1 \qquad \frac{1}{2} \qquad \frac{1}{3} \qquad \frac{-1}{3} \qquad \frac{2}{3} \qquad \frac{4}{3}$$

Si ahora imponemos que $a + b$ *sea un divisor de* 50 *nos quedan únicamente dos posibles raíces, que son* $\frac{-1}{3}$ *y* $\frac{2}{3}$.

	6	11	−19	18	−8
$\frac{-1}{3}$		−2	−3	$\frac{22}{3}$	$\frac{-76}{9}$
	6	9	−22	$\frac{76}{3}$	$\frac{-148}{9}$

	6	11	−19	18	−8
$\frac{2}{3}$		4	10	−6	8
	6	15	−9	12	0

de donde deducimos que $q(x) = \left(x - \frac{2}{3}\right)(6x^3 + 15x^2 - 9x + 12) = (3x - 2)(2x^3 + 5x^2 - 3x + 4)$.

Y ahora podemos concluir que $2x^3 + 5x^2 + 3x + 4$ *no tiene raíces. Por tanto, la única raíz de* $q(x)$ *es* $\frac{2}{3}$.

Terminamos esta sección con un resultado muy sencillo pero que es útil a la hora de estudiar la posible irreducibilidad de polinomios.

Proposición 3.3.4. *Sea* $p(x) \in K[x]$ *un polinomio de grado 2 ó 3. Entonces* $p(x)$ *es irreducible si, y sólo sí, no tiene raíces.*

Demostración: Es claro que si el polinomio es irreducible no tiene raíces, pues en tal caso tendría un divisor de grado uno.

Por otra parte, si el polinomio fuera reducible, vimos que tiene que tener un divisor de grado menor o igual a la mitad del grado de $p(x)$. Por tanto, debe tener un divisor de grado 1, lo que se traduce en que tiene una raíz. ■

Lo dicho en esta proposición vale únicamente para polinomios de grado 2 ó 3. Para polinomios de grado mayor no afirma nada.

Ejemplo 3.3.8.

1. *Sea* $p(x) = x^3 + \frac{5}{2}x^2 - 3x - \frac{3}{2} \in \mathbb{Q}[x]$. *Vamos a estudiar si es reducible o irreducible, y en caso de ser reducible, encontrar su factorización.*

   Como es de grado 3, nos basta con encontrar sus raíces. Para eso, lo que hacemos es trabajar con $q(x) = 2 \cdot p(x) = 2x^3 + 5x^2 - 6x - 3$, *que es primitivo. Las posibles raíces de este polinomio son, en principio,* 1, -1, 3, -3, $\frac{1}{2}$, $\frac{-1}{2}$, $\frac{3}{2}$, $\frac{-3}{2}$.

   Puesto que $q(1) = -2$, *si* $\frac{a}{b}$ *es una raíz de* $q(x)$, $a - b$ *debe ser un divisor de 2. Esto nos elimina las posibilidades* 1, -3, $\frac{-1}{2}$, $\frac{-3}{2}$. *Por tanto, las posibles raíces son* -1, 3, $\frac{1}{2}$ *y* $\frac{3}{2}$.

   Y ahora, dado que $q(-1) = 6$ *podemos descartar* -1, 3 *y* $\frac{3}{2}$. *Luego la única posible raíz es* $\frac{1}{2}$. *Pero* $q(\frac{1}{2}) = \frac{-9}{2} \neq 0$. *Por tanto, el polinomio* $q(x)$ *no tiene raíces y es irreducible (también* $p(x)$*).*

2. *Sea* $p(x) = x^4 + 2x^3 + 2x^2 + 2 \in \mathbb{Z}_3[x]$. *Entonces* $p(0) = 2$, $p(1) = 1$ *y* $p(2) = 0$. *Por tanto, 2 es una raíz y podemos dividir el polinomio por* $x - 2 = x + 1$.

	1	2	2	0	2
2		2	2	2	1
	1	1	1	2	0

   Luego $p(x) = (x+1) \cdot (x^3 + x^2 + x + 2)$. *Este último polinomio es de grado 3 y no tiene raíces (ahora sólo habría que comprobar que 2 no es raíz), lo que nos dice que es irreducible.*

3. *Sea* $p_1(x) = x^4 + 4x^3 + 4x^2 + 3$ *y* $p_2(x) = x^4 + 3x^3 + 3x^2 + x + 4$ *dos polinomios con coeficientes en* $\mathbb{Z}_5$. *Podemos comprobar que ninguno de ellos tiene raíces:*

$p_1(0) = 3$	$p_1(1) = 2$	$p_1(2) = 2$	$p_1(3) = 3$	$p_1(4) = 4$
$p_2(0) = 4$	$p_2(1) = 2$	$p_2(2) = 3$	$p_2(3) = 1$	$p_2(4) = 4$

   Sin embargo, $p_1(x)$ *es reducible, pues puede factorizarse como* $(x^2 + x + 2) \cdot (x^2 + 3x + 4)$, *mientras que* $p_2(x)$ *es irreducible.*

3.3.3. Factores múltiples.

Sabemos que dado un polinomio $p(x) \in K[x]$, ese polinomio se puede expresar de forma única como producto de polinomios irreducibles. En esta factorización puede que aparezca alguno (o algunos) de los irreducibles repetidos. En tal caso, diremos que ese irreducible es un *factor múltiple* de $p(x)$.

Ya vimos (ver definición 44) lo que significa una raíz múltiple. Este concepto puede generalizarse a un polinomio irreducible de cualquier grado.

Definición 48. *Sea* $p(x) \in K[x]$ *y* $q(x) \in K[x]$ *irreducible. Diremos que* $q(x)$ *es un factor de* $p(x)$ *de multiplicidad* m *si* $p(x) = q(x)^m r(x)$ *y* $q(x)$ *no es un divisor de* $r(x)$

Si $q(x)$ *es un factor de multiplicidad mayor o igual que 2, diremos que* $q(x)$ *es un* factor múltiple *de* $p(x)$.

Si $q(x)$ es un factor de $p(x)$ de multiplicidad 1, suele decirse que $q(x)$ es un factor simple de $p(x)$.

Es evidente que es lo mismo decir que a es una raíz de $p(x)$ de multiplicidad m a decir que $(x - a)$ es un factor de $p(x)$ de multiplicidad m.

Ejemplo 3.3.9. *Sea* $p(x) = x^9 + x^8 + x^7 + x^6 + x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$. *Podemos ver que* $x^2 + x + 1$ *es factor de multiplicidad 3, pues* $p(x) = (x^2 + x + 1)^3(x^3 + x + 1)$, *y* $x^2 + x + 1$ *no es un divisor de* $x^3 + x + 1$.

Un polinomio que no tenga factores múltiples es lo que se conoce como *libre de cuadrados.*

Definición 49. *Sea $p(x) \in K[x]$. Se dice que $p(x)$ es libre de cuadrados si no existe $q(x) \in K[x]$, no constante, tal que $q(x)^2 | p(x)$.*

Como ejercicio comprueba que esta definición es equivalente a decir que el polinomio $p(x)$ no tiene factores múltiples.

Lo que vamos a hacer a continuación es tratar de encontrar los factores múltiples de un polinomio. Para esto nos va a ser necesario estudiar la derivada de un polinomio. En este contexto la derivada de un polinomio es una forma de asociarle a un polinomio otro polinomio, pero no tiene ningún sentido de límite, ni de pendiente, etc.

Definición 50. *Sea $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$. Se define la derivada de $p(x)$ como el polinomio*

$$n a_n x^{n-1} + \cdots + 2a_2 x + a_1$$

A dicho polinomio lo denotaremos como $D(p(x))$ o $p'(x)$.

Ejemplo 3.3.10.

1. *Sea $p(x) = 2x^5 - 7x^3 + 3x^2 - 5x + 3 \in \mathbb{Q}[x]$. Entonces $p'(x) = 10x^4 - 21x^2 + 6x - 5$.*
2. *Sea $p(x) = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$. En este caso se tiene que $p'(x) = 0$. Vemos como un polinomio no constante puede tener derivada nula.*

Las propiedades de la derivada de polinomios recuerdan a las conocidas para la derivada de funciones reales. La demostración se deja como ejercicio.

Proposición 3.3.5. *Sean $p(x), q(x) \in K[x]$, y $n \in \mathbb{N}$. Entonces:*

- $D(p(x) + q(x)) = p'(x) + q'(x)$,
- $D(p(x) \cdot q(x)) = p'(x) \cdot q(x) + p(x) \cdot q'(x)$,
- $D(p(x)^n) = n \cdot p(x)^{n-1} p'(x)$.

La importancia de la derivada viene dada por el siguiente resultado.

Proposición 3.3.6. *Sea $p(x) \in K[x]$. Entonces $p(x)$ es libre de cuadrados si, y sólo si, $mcd(p(x), p'(x)) = 1$.*

Demostración:

Demostremos en primer lugar que si $mcd(p(x), p'(x)) = 1$ entonces $p(x)$ es libre de cuadrados, o, equivalentemente, si $p(x)$ no es libre de cuadrados entonces $mcd(p(x), p'(x)) \neq 1$.

Si $p(x)$ no es libre de cuadrados, entonces existen $q(x), r(x) \in K[x]$ tales que $p(x) = q(x)^2 r(x)$. Se tiene entonces que

$$p'(x) = D(q(x)^2) r(x) + q(x)^2 D(r(x)) = 2q(x)q'(x)r(x) + q(x)r'(x) = q(x)\big(2q'(x)r(x) + q(x)r'(x)\big),$$

lo que implica que $q(x) | p'(x)$, y como $q(x) | p(x)$ se tiene que $q(x) | mcd(p(x), p'(x))$.

Recíprocamente, supongamos que $mcd(p(x), p'(x)) \neq 1$. Sea entonces $q(x)$ un polinomio irreducible divisor de $mcd(p(x), p'(x))$. Se tiene entonces que $p(x) = q(x)r(x)$. Derivamos:

$$p'(x) = q'(x)r(x) + q(x)r'(x)$$

Dado que $q(x) | p'(x)$ y $q(x) | q(x)r'(x)$ deducimos que $q(x) | q'(x)r(x)$, y al ser $q(x)$ irreducible tenemos dos opciones:

- $q(x)|r(x)$. En este caso $r(x) = q(x)h(x)$, de donde $p(x) = q(x)^2h(x)$, es decir, $p(x)$ no es libre de cuadrados.
- $q(x)|q'(x)$. Pero esta posibilidad sólo podría darse si $q'(x) = 0$. Sin embargo, veremos en un capítulo posterior que si $q'(x) = 0$ entonces $q(x)$ no es irreducible.

■

Corolario 3.3.1. *Sea $p(x) \in K[x]$ y $a \in K$ una raíz de $p(x)$. Entonces a es una raíz múltiple de $p(x)$ si, y sólo si, $p'(a) = 0$.*

Ejemplo 3.3.11.

1. *Hemos visto que el polinomio $p(x) = x^9+x^8+x^7+x^6+x^5+x^2+1 \in \mathbb{Z}_2[x]$ no es libre de cuadrados, pues tenía un factor triple. Su derivada vale $p'(x) = x^8 + x^6 + x^4$. Vamos a calcular el máximo común divisor de $p(x)$ y su derivada. Para ello, usaremos el algoritmo de Euclides.*

   $x^9 + x^8 + x^7 + x^6 + x^5 + x^2 + 1 = (x^8 + x^6 + x^4) \cdot (x + 1) + x^4 + x^2 + 1.$

   $x^8 + x^6 + x^4 = (x^4 + x^2 + 1) \cdot x^4 + 0.$

   Por tanto, $mcd(p(x), p'(x)) = x^4 + x^2 + 1 \neq 1$.

2. *Sea $p(x) = x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$. Entonces $p'(x) = x^8 + x^4 + x^2$. Para calcular el máximo común divisor de $p(x)$ y $p'(x)$ empleamos el algoritmo de Euclides.*

   En este caso, como la única posibilidad para a es que valga uno, no pondremos esa columna.

$p(x)$	$q(x)$
$x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$	$x^8 + x^4 + x^2$
$x^8 + x^4 + x^2$	$x^6 + x^2 + 1$
$x^6 + x^2 + 1$	0

   luego $mcd(p(x), p'(x)) = x^6 + x^2 + 1$. De hecho,

   $$p(x) = (x^6 + x^2 + 1)(x^3 + x^2 + 1) \qquad p'(x) = (x^6 + x^2 + 1)x^2$$

   Si $q(x) = x^6 + x^2 + 1$ se tiene que $q'(x) = 0$. Nótese que $q(x)$ no es irreducible, pues $q(x) = (x^3 + x + 1)^2$.

   La factorización de $p(x)$ es $p(x) = (x^3 + x + 1)^2(x^3 + x^2 + 1)$.

3. *Sea $p(x) = x^7 + 2x^6 + x^5 + x^4 + x + 2 \in \mathbb{Z}_3[x]$. Su derivada vale $p'(x) = x^6 + 2x^4 + x^3 + 1$. Vamos a calcular $mcd(p(x), p'(x))$.*

a	$p(x)$	$q(x)$
	$x^7 + 2x^6 + x^5 + x^4 + x + 2$	$x^6 + 2x^4 + x^3 + 1$
	$x^6 + 2x^4 + x^3 + 1$	$2x^5 + 2x^4 + x^3$
	$2x^5 + 2x^4 + x^3$	$x^4 + 1$
	$x^4 + 1$	$x^3 + x + 1$
	$x^3 + x + 1$	$2x^2 + 2x + 1$
2	$2x^2 + 2x + 1$	0
	$\mathbf{x^2 + x + 2}$	

   Es decir, $mcd(p(x), p'(x)) = x^2 + x + 2$

   A partir de esto es fácil ver que la factorización de $p(x)$ es $(x^2 + x + 2)^2(x^3 + 2x + 2)$.

Vemos por tanto, que para encontrar los factores múltiples de un polinomio lo que hay que hacer es calcular el máximo común divisor del polinomio y su derivada.

3.3.4. Factorización de polinomios en $\mathbb{Z}_p[x]$

Ya comentamos la existencia de un algoritmo (algoritmo de Berlekamp) para factorizar polinomios con coeficientes en $\mathbb{Z}_p$. Pero nosotros aquí, lo único que vamos a hacer es ir probando por los distintos irreducibles para ver si encontramos un divisor de un polinomio.

Supongamos entonces que tenemos un polinomio $q(x) \in \mathbb{Z}_p[x]$ de grado n. Si el polinomio es reducible, entonces tiene un factor irreducible de grado menor o igual que $\frac{n}{2}$.

Comprobamos en primer lugar si tiene o no divisores de grado 1, es decir, comprobamos si tiene raíces. A continuación comprobamos si tiene divisores irreducibles de grado 2, y así sucesivamente.

Ejemplo 3.3.12.

1. *Sea $q(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Al ser de grado 3 únicamente hay que comprobar si tiene o no raíces. Puesto que $q(0) = q(1) = 1$ podemos deducir que el polinomio es irreducible. De la misma forma se comprueba que $x^3 + x^2 + 1$ es irreducible.*

2. *Sea ahora $q(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$. En este caso $q(0) = q(1) = 1$, luego no tiene ningún divisor de grado 1.*

   Probamos a dividir por $x^2 + x + 1$, que es irreducible de grado 2, y nos queda que $x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$. Los dos polinomios que aparecen son irreducibles (pues no tienen raíces).

3. *Sea $q(x) = x^7 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$. Entonces:*

   Evaluamos en $x = 0$ y $x = 1$. En ambos casos nos sale 1, luego $q(x)$ no tiene divisores de grado 1.

   Dividimos por $x^2 + x + 1$, y nos queda $q(x) = (x^2 + x + 1)(x^5 + x^4 + x + 1) + x$. Por tanto no tiene divisores de grado 2.

   Dividimos por $x^3 + x + 1$ y $x^3 + x^2 + 1$. En el primer caso nos queda $q(x) = (x^3 + x + 1)(x^4 + x^2) + (x^2 + x + 1)$ y en el segundo $q(x) = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + x + 1)$.

   Puesto que $x^4 + x^3 + x^2 + x + 1$ no tiene divisores de grado 1 y grado 2 (ya que de tenerlos serían también divisores de $q(x)$ deducimos que $x^4 + x^3 + x^2 + x + 1$ es irreducible.

   La factorización de $q(x)$ como producto de irreducibles es

$$x^7 + x^4 + x^3 + x + 1 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + x + 1).$$

Como vemos, para factorizar un polinomio en $\mathbb{Z}_p[x]$ es conveniente conocer los polinomios irreducibles mónicos de grado bajo, pues son por los que hemos de efectuar las divisiones. A continuación calcularemos algunos de estos irreducibles.

1. Polinomios irreducibles en $\mathbb{Z}_2[x]$

   - Grado 1. Aquí, los irreducibles son todos, es decir,

$$x \qquad x + 1.$$

   - Grado 2. Los no irreducibles son x^2, $x(x + 1) = x^2 + x$ y $(x + 1)(x + 1) = x^2 + 1$. El único que queda es

$$x^2 + x + 1.$$

   - Grado 3. También aquí los únicos que hay son los que no tienen raíces. Estos son:

$$x^3 + x + 1 \qquad x^3 + x^2 + 1.$$

   - Grado 4. Aquí hemos de eliminar todos los que tengan raíces y $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Nos quedan entonces tres polinomios, que son:

$$x^4 + x + 1 \qquad x^4 + x^3 + 1 \qquad x^4 + x^3 + x^2 + x + 1.$$

- Grado 5. Los reducibles son los que tienen raíces y los dos que toman una factorización de la forma (grado 2) · (grado 3). Estos dos son $(x^2+x+1)(x^3+x+1) = x^5+x^4+1$ y $(x^2+x+1)(x^3+x^2+1) = x^5+x+1$.

  Nos quedan entonces 6 polinomios que son:

$$x^5+x^2+1 \qquad x^5+x^3+1 \qquad x^5+x^4+x^3+x^2+1 \qquad x^5+x^4+x^3+x+1$$

$$x^5+x^4+x^2+x+1 \qquad\qquad x^5+x^3+x^2+x+1.$$

2. Polinomios mónicos irreducibles en $\mathbb{Z}_3[x]$.

   - Grado 1. Al igual que antes, todos son irreducibles. Tenemos por tanto

$$x \qquad x+1 \qquad x+2.$$

   - Grado 2. Son aquellos que no tiene raíces. Hay un total de 3, que son:

$$x^2+1 \qquad x^2+x+2 \qquad x^2+2x+2.$$

   - Grado 3. Son también los que no tienen raíces. En este caso hay 8.

$$x^3+2x+1 \qquad x^3+2x+2 \qquad x^3+x^2+2 \qquad x^3+2x^2+1$$

$$x^3+x^2+x+2 \qquad x^3+x^2+2x+1 \qquad x^3+2x^2+x+1 \qquad x^3+2x^2+2x+2.$$

   - De grado 4 hay 18 polinomios irreducibles.

3. Polinomios mónicos irreducibles en $\mathbb{Z}_5[x]$.

   - Grado 1. Tenemos 5 irreducibles:

$$x \qquad x+1 \qquad x+2 \qquad x+3 \qquad x+4.$$

   - Grado 2. Los que no tienen raíces son 10.

$$x^2+2 \qquad x^2+3 \qquad x^2+x+1 \qquad x^2+x+2 \qquad x^2+2x+3$$

$$x^2+2x+4 \qquad x^2+3x+3 \qquad x^2+3x+4 \qquad x^2+4x+1 \qquad x^2+4x+2.$$

   - Para grados mayores el número de polinomios es muy grande. Así, de grado 3 la lista tendría 40 polinomios, mientras que la de grado 4 sería de 150.

4. Polinomios mónicos irreducibles en $\mathbb{Z}_7[x]$.

   - Grado 1. Como siempre aquí son todos irreducibles.

$$x \qquad x+1 \qquad x+2 \qquad x+3 \qquad x+4 \qquad x+5 \qquad x+6.$$

   - Grado 2. Aquí la lista es ya muy grande. Tenemos un total de 21 polinomios.

$$x^2+1 \quad x^2+2 \quad x^2+4 \quad x^2+x+3 \quad x^2+x+4 \quad x^2+x+6 \quad x^2+2x+2$$

$$x^2+2x+3 \quad x^2+2x+5 \quad x^2+3x+1 \quad x^2+3x+5 \quad x^2+3x+6 \quad x^2+4x+1 \quad x^2+4x+5$$

$$x^2+4x+6 \quad x^2+5x+2 \quad x^2+5x+3 \quad x^2+5x+5 \quad x^2+6x+3 \quad x^2+6x+4 \quad x^2+6x+6.$$

   - De grado 3 hay un total de 112 polinomios irreducibles.

3.3.5. Factorización de polinomios con coeficientes enteros o racionales.

El lema de Gauss

En este apartado vamos a desarrollar una idea que ya hemos mencionado previamente. La relación entre la factorización de polinomios con coeficientes en $\mathbb{Z}$ y $\mathbb{Q}$.

El resultado clave es el que da nombre a la sección: el lema de Gauss.

Recordemos que el contenido de un polinomio con coeficientes enteros se definía como el máximo común divisor de sus coeficientes.

Lema 3.3.1 (Lema de Gauss)**.** *Sean $q_1(x), q_2(x) \in \mathbb{Z}[x]$ dos polinomios primitivos. Entonces $q_1(x) \cdot q_2(x)$ es primitivo.*

Demostración: Supongamos que $q_1(x) \cdot q_2(x)$ no es primitivo. Entonces $c(q_1(x) \cdot q_2(x)) \neq 1$. Sea entonces p un primo que divide a $c(q_1(x) \cdot q_2(x))$.

Supongamos también que $q_1(x) = a_n x^n + \cdot + a_1 x + a_0$ y que $q_2(x) = b_m x^m + \cdots + b_1 x + b_0$. Puesto que $q_1(x)$ es primitivo, debe existir un coeficiente que no sea múltiplo de p. Supongamos que el primero de ellos es a_k. De la misma forma, sea b_l el primer coeficiente de $q_2(x)$ que no es múltiplo de p. Entonces el coeficiente de grado $k+l$ del polinomio $q_1(x) \cdot q_2(x)$ es

$$a_0 b_{k+l} + \cdots + a_{k-1} b_{l+1} + a_k b_l + a_{k+1} b_{l-1} + \cdots + a_{k+l} b_0$$

Puesto que $a_0, \cdots a_{k-1}$ son todos múltiplos de p se tiene que $a_0 b_{k+l} + \cdots + a_{k-1} b_{l+1}$ es múltiplo de p. Puesto que $b_0, \cdots b_{l-1}$ son múltiplos de p también lo es $a_{k+1} b_{l-1} + \cdots + a_{k+l} b_0$, y como el término de grado $k+l$ de $q_1(x) \cdot q_2(x)$ es múltiplo de p deducimos que $a_k b_l$ es múltiplo de p, lo cual no es posible, pues ni a_k ni b_l lo son (recordemos la proposición 2.5.1). ■

Corolario 3.3.2. *Sean $p(x), q(x) \in \mathbb{Z}[x]$. Entonces $c(p(x) \cdot q(x)) = c(p(x)) \cdot c(q(x))$.*

Demostración: Se tiene que $p(x) = c(p(x)) \cdot p_1(x)$ y $q(x) = c(q(x)) \cdot q_1(x)$, donde $p_1(x)$ y $q_1(x)$ son primitivos. Entonces

$$p(x) \cdot q(x) = [c(p(x)) \cdot p_1(x)] \cdot [c(q(x)) \cdot q_1(x)] = [c(p(x)) \cdot c(q(x))] \cdot p_1(x) \cdot q_1(x)$$

y como $p_1(x) \cdot q_1(x)$ es primitivo deducimos que

$$c(p(x) \cdot q(x)) = c(p(x)) \cdot c(q(x))$$

■

Ejemplo 3.3.13.

1. *Sean $p(x) = 3x^6 + 5x^5 - 4x^4 + 6x^3 - 10x^2 + 10x - 20$ y $q(x) = 2x^5 + 15x^4 - 12x^3 + 8x^2 - 18x + 12$. Claramente, ambos polinomios son primitivos. Si los multiplicamos nos queda*

					3	5	−4	6	−10	10	−20
						2	15	−12	8	−18	12
					36	60	−48	82	−120	120	−240
				−54	−90	72	−108	180	−180	−360	
			24	40	−32	48	−80	80	−160		
		−36	−60	48	−72	120	−120	240			
	45	75	−60	90	−150	150	−300				
6	10	−8	12	−20	20	−40					
6	55	31	−84	104	−234	410	−656	572	−460	−240	−240

es decir,

$$p(x) \cdot q(x) = 6x^{11} + 55x^{10} - 31x^9 - 84x^8 + 104x^7 - 234x^6 + 410x^5 - 656x^4 + 572x^3 - 460x^2 - 240x - 240$$

que también es primitivo.

Si analizamos los coeficientes, vemos que el primer coeficiente de $p(x)$ que no es múltiplo de 2 es el de grado 5 ($5x^5$), mientras que el primero de $q(x)$ que no es de múltiplo de 2 es el de grado 4 ($15x^4$). Al multiplicar los dos polinomios, el primer coeficiente que no es múltiplo de 2 es el de grado 9. Podemos apreciar como todos los sumandos que intervienen en los términos de grado menor o igual que 8 son múltiplos de 2, mientras que en los que intervienen en el de grado 9 todos son múltiplos de 2 salvo uno.

2. *El polinomio $2x^2+6x-4$ tiene contenido igual a 2, mientras que el polinomio $12x^2-18x+30$ tiene contenido igual a 6. Su producto, que es $24x^4-108x^3-96x^2+252x-120$ tiene contenido igual a 12.*

Teorema 3.3.3. *Sea $p(x) \in \mathbb{Z}[x]$ no constante. Entonces $p(x)$ es irreducible en $\mathbb{Z}[x]$ si, y sólo si, $p(x)$ es primitivo y es irreducible en $\mathbb{Q}[x]$.*

Demostración: Sea $p(x) \in \mathbb{Z}[x]$ y supongamos que es irreducible. Claramente es primitivo, pues en caso contrario tendríamos que $c(p(x))|p(x)$.

Si el polinomio fuera reducible en $\mathbb{Q}[x]$ tendríamos una factorización en $\mathbb{Q}[x]$ de la forma $p_1(x)\cdot p_2(x)$. Ahora bien, $p_1(x)=\frac{a}{b}q_1(x)$ y $p_2(x)=\frac{c}{d}q_2(x)$ con $q_1(x),q_2(x)\in\mathbb{Z}[x]$ primitivos. Entonces

$$p(x)=\frac{ac}{bd}q_1(x)q_2(x)$$

Como tanto $p(x)$ como $q_1(x)q_2(x)$ son primitivos, deducimos que $\frac{ac}{bd}=1$ (o $\frac{ac}{bd}=-1$) lo que nos dice que $p(x)=q_1(x)q_2(x)$ es una factorización en $\mathbb{Z}[x]$, en contra de la hipótesis de que $p(x)$ es irreducible.

Recíprocamente, si $p(x)$ es primitivo e irreducible en $\mathbb{Q}[x]$, si tuviera algún divisor propio en $\mathbb{Z}[x]$ éste no podría ser un polinomio constante, luego sería también un divisor propio en $\mathbb{Q}[x]$. ■

Ejemplo 3.3.14.

1. *Sea $p(x)=6x-4\in\mathbb{Z}[x]$. Visto como polinomio en $\mathbb{Q}[x]$ es irreducible, pues es de grado 1. Sin embargo, en $\mathbb{Z}[x]$ no es irreducible, pues $2|(6x-4)$ y $(3x-2)|(6x-4)$.*

2. *Sea $p(x)=6x^3-19x^2-8x+12$. Podemos ver que este polinomio no es irreducible en $\mathbb{Q}[x]$, pues $x=\frac{2}{3}$ es una raíz, ya que*

$$p\left(\frac{2}{3}\right)=6\left(\frac{2}{3}\right)^3-19\left(\frac{2}{3}\right)^2-8\frac{2}{3}+12=6\frac{8}{27}-19\frac{4}{9}-8\frac{2}{3}+12=\frac{16}{9}-\frac{76}{9}-\frac{48}{9}+\frac{108}{9}=0$$

Dividimos por $x-\frac{2}{3}$

	6	−19	−8	12
$\frac{2}{3}$		4	−10	−12
	6	−15	−18	0

luego $p(x)=\left(x-\frac{2}{3}\right)(6x^2-15x-18)=\left[\frac{1}{3}(3x-2)\right]\cdot[3\cdot(2x^2-5x-6)]=(3x-2)(2x^2-5x-6)$

Vemos como el polinomio es reducible en $\mathbb{Z}[x]$.

Dejamos anteriormente la demostración de la proposición 3.3.3. Recordemos que esta proposición decía que si $p(x)$ es un polinomio primitivo y $\frac{a}{b}$ es una raíz racional de $p(x)$ tal que $mcd(a,b)=1$ entonces para cualquier número entero c se tiene que $(bc-a)$ es un divisor de $p(c)$.

Ahora podemos demostrarla. Por ser $\frac{a}{b}$ una raíz racional, se tiene que $p(x)=\left(x-\frac{a}{b}\right)\cdot p_1(x)$. Es fácil ver ahora que el contenido del polinomio $p_1(x)$ vale b (¿por qué?), luego el polinomio $\frac{p_1(x)}{b}$ tiene los coeficientes enteros, y para cualquier número entero c, $\frac{p_1(c)}{b}\in\mathbb{Z}$. Se tiene la siguiente factorización en $\mathbb{Z}[x]$.

$$p(x)=(bx-a)\cdot\frac{p_1(x)}{b},\ \text{luego } p(c)=(bc-a)\cdot\frac{p_1(c)}{b}$$

Es decir, $p(c)$ es múltiplo de $bc-a$.

Criterios de irreducibilidad.

Hemos visto que, salvo constantes, los polinomios irreducibles en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$ son los mismos. Vamos a continuación a dar unos criterios que nos van a permitir asegurar que un polinomio primitivo con coeficientes en $\mathbb{Z}$ es irreducible (y por tanto, que un polinomio con coeficientes en $\mathbb{Q}$ es irreducible). Estos criterios **nunca** nos sirven para afirmar que un polinomio es reducible.

Proposición 3.3.7 (Criterio de Eisenstein). *Sea $q(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ primitivo. Supongamos que existe un número primo p tal que $p|a_i : i = 0, 1, \ldots, n-1$ y $p^2 \not| a_0$. Entonces $q(x)$ es irreducible.*

Demostración: Hagamos la demostración por reducción al absurdo. Supongamos entonces que $q(x)$ fuera reducible. Entonces tendríamos una factorización de la forma

$$q(x) = (b_m x^m + \cdots + b_1 x + b_0)(c_k x^k + \cdots + c_1 x + c_0).$$

Puesto que $a_0 = b_0 c_0$, deducimos que $p|b_0 c_0$, luego p divide a uno de los dos coeficientes. Además no puede dividir a los dos, pues en ese caso tendríamos que $p^2|a_0$. Suponemos, por ejemplo, que $p|b_0$ (y por tanto que $p \not| c_0$).

Supongamos ahora que $p|b_0,\ p|b_1, \cdots, p|b_i$. Vamos a demostrar que $p|b_{i+1}$. Se tiene que

$$a_{i+1} = b_0 c_{i+1} + b_1 c_i + \cdots + b_i c_1 + b_{i+1} c_0.$$

Todos los sumandos, salvo quizá el último son múltiplos de p. También la suma total (a_{i+1}) es múltiplo de p. Por tanto, tenemos que $b_{i+1} c_0$ es múltiplo de p. Como c_0 no lo es, deducimos que b_{i+1} es múltiplo de p.

De esta forma demostramos que todos los coeficientes de $b_m x^m + \cdots + b_1 x + b_0$ son múltiplos de p, lo que implicaría que $a_n = b_m c_k$ sería múltiplo de p, lo cual no es posible. ■

Ejemplo 3.3.15.

1. *El polinomio $x^2 + 4x + 4$ satisface todas las hipótesis del criterio de Eisenstein para el primo $p = 2$ salvo la que afirma que $p^2 \not| a_0$. Vemos que este polinomio es reducible, pues $x^2 + 4x + 4 = (x+2)^2$.*
2. *El polinomio $x^2 + 4x + 8$ satisface también todas las hipótesis del criterio de Eisenstein para el primo $p = 2$ salvo la que afirma que $p^2 \not| a_0$. En este caso el polinomio es irreducible.*
3. *El polinomio $5x^5 + 6x^4 - 12x^2 + 18x - 24$ satisface las hipótesis del criterio de Eisenstein para $p = 3$. Por tanto es irreducible. Nótese que para $p = 2$ no es posible aplicar el criterio.*
4. *Para cualquier primo p, los polinomios $x^n + p$ y $x^n - p$ son irreducibles.*

Los dos primeros ejemplos nos dicen que si suprimimos una de las hipótesis del criterio de Eisenstein, no podemos afirmar nada sobre el polinomio, pues en el primer caso es reducible y en el segundo es irreducible.

Proposición 3.3.8. *[Reducción módulo un primo] Sea $q(x) \in \mathbb{Z}[x]$, y p un número primo. Denotemos por $\overline{q}(x)$ al polinomio en $\mathbb{Z}_p[x]$ cuyos coeficientes son los de $q(x)$ que se han reducido módulo p. Entonces, si $gr(\overline{q}(x)) = gr(q(x))$ y $\overline{q}(x)$ es irreducible podemos asegurar que $q(x)$ es irreducible.*

Este criterio se suele enunciar diciendo que si $q(x)$ es irreducible en $\mathbb{Z}_p[x]$ entonces $q(x)$ es irreducible en $\mathbb{Z}[x]$.

Demostración: Demostraremos el contrarrecíproco, es decir, si $q(x)$ es reducible en $\mathbb{Z}[x]$ entonces $\overline{q}(x)$ es reducible en $\mathbb{Z}_p[x]$.

Ahora bien, si $q(x)$ es reducible en $\mathbb{Z}[x]$ se tiene que $q(x) = q_1(x) \cdot q_2(x)$, de donde $\overline{q}(x) = \overline{q_1}(x) \cdot \overline{q_2}(x)$ en $\mathbb{Z}_p[x]$. Esta última afirmación es cierta pues si $a_i = b_0 c_i + \cdots + b_i c_0$ en $\mathbb{Z}$ entonces $a_i = b_0 c_i + \cdots + b_i c_0$ en $\mathbb{Z}_p$ para cualquier primo p.

Tenemos por tanto que toda factorización en $\mathbb{Z}[x]$ da lugar a una factorización en $\mathbb{Z}_p[x]$. ■

Aunque no se haya mencionado en la demostración, la hipótesis de que $gr(q(x)) = gr(\overline{q}(x))$ es importante. Analiza en que momento de la demostración es necesaria. En el siguiente ejemplo puedes encontrar alguna ayuda.

En lo que sigue, denotaremos por $q(x)$ tanto al polinomio con coeficientes en $\mathbb{Z}$ como al polinomio con coeficientes en $\mathbb{Z}_p$.

Ejemplo 3.3.16.

1. *Sea* $q(x) = 2x^3 - 15x^2 + 19x - 7$. *Si reducimos el polinomio módulo* 2 *nos queda* $q(x) = x^2 + x + 1$, *que sabemos que es irreducible. Sin embargo,* $q(x)$ *es reducible, pues* $q(x) = (2x - 1)(x^2 - 5x + 7)$.

2. *El polinomio* $x^5 + 4x^4 - 7x^3 + 12x^2 - 10x + 9$ *es irreducible en* $\mathbb{Z}[x]$, *y por tanto en* $\mathbb{Q}[x]$ *pues al reducirlo módulo* 2 *nos queda* $x^5 + x^3 + 1$, *que es irreducible.*

3. *Consideramos el polinomio* $x^4-4x^3+3x^2+7x-5$. *Si lo reducimos módulo* 2 *nos queda* x^4+x^2+x+1 *que es reducible, pues* $x = 1$ *es una raíz. De hecho* $x^4 + x^2 + x + 1 = (x + 1)(x^3 + x^2 + 1)$

   Si reducimos módulo 3 *nos queda* $q(x) = x^4+2x^3+x+1$. *Evaluamos* $q(x)$ *en los diferentes puntos de* $\mathbb{Z}_3$ *y comprobamos que no tiene raíces (*$q(0) = 1$, $q(1) = 2$, $q(2) = 2$*). Dividimos por los polinomios irreducibles de grado* 2, *y nos sale:*

   $$x^4 + 2x^3 + x + 1 = (x^2 + 1)(x^2 + 2x + 2) + 2x + 2$$
   $$x^4 + 2x^3 + x + 1 = (x^2 + x + 2)(x^2 + x) + x + 1$$

   Por tanto $q(x)$ *es irreducible en* $\mathbb{Z}_3$. *Deducimos entonces que* $x^4 - 4x^3 + 3x^2 + 7x - 5$ *es irreducible en* $\mathbb{Z}[x]$.

4. *El polinomio* $q(x) = x^5 + 3x^4 + 3x^3 - 4x + 3$ *es reducible en* $\mathbb{Z}[x]$ *y su factorización como producto de irreducibles es* $(x^2 + 2x + 3)(x^3 + x^2 - 2x + 1)$. *Si lo reducimos módulo* 2 *nos queda*

   $q(x) = x^5 + x^4 + x^3 + 1 = (x + 1)^2(x^3 + x^2 + 1)$

   Obviamente, al reducir $q(x)$ *módulo* 2 *nos debe quedar un polinomio reducible. Además, la factorización que tenemos en* $\mathbb{Z}[x]$ *pasa a una factorización en* $\mathbb{Z}_2[x]$. *Los factores puede ocurrir que sean reducibles módulo* 2. *En el caso que nos ocupa, uno de los factores (*$x^2 + 2x + 3$*) es reducible (*$x^2+2x+3 = x^2+1 = (x+1)^2$*), mientras que el otro (*$x^3+x^2-2x+1 = x^3+x^2+1$*) es irreducible.*

5. *Tomamos el polinomio* $q(x) = x^4 + 1 \in \mathbb{Z}[x]$.

   Este polinomio en $\mathbb{Z}_2[x]$ *es reducible. Su factorización es* $q(x) = (x + 1)^4$.

   En $\mathbb{Z}_3[x]$ *es también reducible. Su factorización es* $q(x) = (x^2 + x + 2)(x^2 + 2x + 2)$.

   En $\mathbb{Z}_5[x]$ *es también reducible. Su factorización es* $q(x) = (x^2 + 2)(x^2 + 3)$.

   En $\mathbb{Z}_7[x]$ *es reducible. Su factorización es* $q(x) = (x^2 + 3x + 1)(x^2 + 4x + 1)$.

   En $\mathbb{Z}_{11}[x]$ *es reducible. Su factorización es* $q(x) = (x^2 + 3x + 10)(x^2 + 8x + 10)$.

   En $\mathbb{Z}_{13}[x]$ *es reducible. Su factorización es* $q(x) = (x^2 + 5)(x^2 + 8)$.

   En $\mathbb{Z}_{17}[x]$ *es reducible. Su factorización es* $q(x) = (x + 2)(x + 8)(x + 9)(x + 15)$.

   En general, para cualquier primo p, *el polinomio* $q(x) = x^4 + 1$ *es reducible en* $\mathbb{Z}_p[x]$. *Sin embargo,* $q(x)$ *es irreducible en* $\mathbb{Z}[x]$ *y en* $\mathbb{Q}[x]$. *Para comprobarlo, podemos calcular su factorización como producto de irreducibles en* $\mathbb{R}[x]$, *que es* $q(x) = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$, *y ninguno de ellos tiene sus coeficientes en* $\mathbb{Q}$.

   Por tanto, en el caso de que el polinomio $q(x)$ *sea reducible en* $\mathbb{Z}_p[x]$, *no podemos afirmar nada sobre la reducibilidad o irreducibilidad de* $q(x)$.

Este método, en principio sólo puede ser aplicado cuando encontramos un primo p donde el polinomio de partida es irreducible en $\mathbb{Z}_p[x]$. Sin embargo, profundicando un poco más en la idea que subyace a este criterio (toda factorización en $\mathbb{Z}[x]$ se mantiene al reducir el polinomio módulo p) podemos afinar algo más a la hora de aplicar el criterio. Antes de explicar como funcionaría veremos algunos ejemplos.

Ejemplo 3.3.17.

1. *Sea* $q(x) = x^4 - 2x^3 + 3x^2 + x - 1$. *Reducimos módulo* 2 *y factorizamos:*

$$x^4 + x^2 + x + 1 = (x + 1)(x^3 + x^2 + 1)$$

y en principio no podemos deducir nada. Reducimos entonces módulo 3.

$$x^4 + x^3 + x + 2 = (x^2 + 1)(x^2 + x + 2)$$

y el polinomio resulta ser también reducible.

Ahora bien, si $q(x)$ *fuera reducible, la factorización suya se mantendría al reducir* $q(x)$ *módulo* 2. *Puesto que en* $\mathbb{Z}_2[x]$ *se tiene que* $q(x)$ *es producto de un polinomio de grado* 1 *por uno de grado* 3 *deducimos que si* $q(x)$ *es reducible, entonces se factoriza como un polinomio de grado* 1 *por uno de grado* 3.

Pero también la factorización de $q(x)$ *se mantendría al reducirlo módulo* 3. *Sin embargo, en* $\mathbb{Z}_3[x]$, *el polinomio* $q(x)$ *no tiene ninguna raíz, luego no podemos tener una factorización de* $q(x)$ *de la forma (grado* 1*)·(grado* 3*).*

Deducimos entonces que $q(x)$ *es irreducible.*

En este caso se dice que las factorizaciones de $q(x)$ *módulo* 2 *y módulo* 3 *son incompatibles.*

2. *En el ejemplo precedente, una vez vista la factorización en* $\mathbb{Z}_2[x]$ *bastaría comprobar que no tiene raíces en* $\mathbb{Q}$. *Puesto que* $q(1) = 2$ *y* $q(-1) = 4$ *podemos deducir que* $q(x)$ *es irreducible.*

3. *Sea* $q(x) = x^4 + 4x^3 + 6x^2 + x - 4$. *Si reducimos módulo* 2 *obtenemos:*

$$x^4 + x = x(x + 1)(x^2 + x + 1)$$

mientras que al reducir módulo 3 *nos da*

$$x^4 + x^3 + x + 2 = (x^2 + 1)(x^2 + x + 2)$$

En este caso tenemos dos factorizaciones distintas, sin embargo no son incompatibles, pues en ambos casos tenemos una posible factorización (grado 2*)·(grado* 2*).*

De hecho, este polinomio es reducible, pues $x^4 + 4x^3 + 6x^2 + x - 4 = (x^2 + 3x + 4)(x^2 + x - 1)$.

Definición 51. *Sea* $q(x) \in \mathbb{Z}[x]$, *y* p *un número primo tal que al reducir* $q(x)$ *módulo* p *no disminuye el grado. Definimos el conjunto* D_p *(o* $D_p(q(x))$*) como el conjunto formado por los grados de los divisores propios de* $q(x)$ *en* $\mathbb{Z}_p[x]$.

Si $p_1, \cdots, p_k$ *son números primos, se define el conjunto* $D_{p_1,\cdots,p_k}$ *como*

$$D_{p_1,\cdots,p_k} = D_{p_1} \cap \cdots \cap D_{p_k}$$

Ejemplo 3.3.18.

1. *Si* $q(x) = x^4 - 2x^3 + 3x^2 + x - 1$ *entonces* $D_2 = \{1, 3\}$, *pues sus divisores son* $x + 1$ *y* $x^3 + x^2 + 1$, *que tienen grados* 1 *y* 3 *respectivamente. Por otra parte,* $D_3 = \{2\}$, *pues cualquier divisor suyo tiene grado* 2.

   Por tanto se tiene que $D_{2,3} = \emptyset$.

2. *Si* $q(x) = x^4 + 4x^3 + 6x^2 + x - 4$ *entonces* $D_2 = \{1, 2, 3\}$.

   Son divisores de grado 1, x *y* $x + 1$.

   Son divisores de grado 2, $x(x + 1)$ *y* $x^2 + x + 1$.

   Son divisores de grado 3, $x(x^2 + x + 1)$ *y* $(x + 1)(x^2 + x + 1)$.

   Mientras que $D_3 = \{2\}$. *Por tanto* $D_{2,3} = \{2\}$.

Claramente se tiene que $q(x)$ es irreducible en $\mathbb{Z}_p[x]$ si, y sólo si, $D_p = \emptyset$.

Por otra parte, se tiene que si existen primos $p_1, \ldots, p_k$ tales que $D_{p_1,\ldots,p_k} = \emptyset$ entonces $q(x)$ es irreducible.

Sin embargo, aunque esto mejora a la proposición 3.3.8, en algunos casos puede no servirnos para deducir si un polinomio es reducible o irreducible. Por ejemplo, hemos visto que $x^4 + 1$ es irreducible, y sin embargo, $2 \in D_{2,3,5,7,11,13,17}$. De hecho, para cualquier primo p se tiene que $2 \in D_p(x^4 + 1)$.

3.4. Anillos cocientes de polinomios. Cuerpos finitos

En los capítulos anteriores, dado un número natural $n \geq 2$, construimos el conjunto $\mathbb{Z}_n$, y después definimos su aritmética.

Ahora, sustituimos $\mathbb{Z}$ por $K[x]$, con K un cuerpo. Si $m(x) \in K[x]$ vamos a definir el conjunto $K[x]_{m(x)}$. Para esto, necesitamos definir la relación de congruencia entre polinomios, de forma análoga a como se hizo con números enteros.

Definición 52. *Sea K un cuerpo y $a(x), b(x), m(x) \in K[x]$. Se dice que $a(x)$ es congruente con $b(x)$ módulo $m(x)$, y se escribe $a(x) \equiv b(x)(\text{mód } m(x))$ si $m(x)|(b(x) - a(x))$. Es decir:*

$$a(x) \equiv b(x)(\text{mód } m(x)) \text{ si existe } c(x) \in K[x] \text{ tal que } b(x) - a(x) = c(x)m(x).$$

Nótese que la relación de congruencia módulo 0 es la relación de igualdad ($a(x) \equiv b(x)(\text{mód } 0)$ si, y sólo si, $a(x) = b(x)$), mientras que si $\lambda \in K^*$ entonces $a(x) \equiv b(x)(\text{mód } \lambda)$ cualesquiera que sean $a(x)$ y $b(x)$. Por tanto, nos centraremos en congruencias módulo $m(x)$ con $m(x)$ un polinomio de grado mayor o igual que 1.

Además, se tiene que $a(x) \equiv b(x)(\text{mód } m(x))$ si, y sólo si, $a(x) \equiv b(x)(\text{mód } \lambda \cdot m(x))$, donde $\lambda \in K^*$. Por tanto, al hablar de congruencias módulo $m(x)$ podemos suponer que $m(x)$ es un polinomio mónico.

Ejemplo 3.4.1. *Sea $m(x) = x^2 + 2 \in \mathbb{Z}_3[x]$. Entonces:*

$$x^4 + 2x^3 + x^2 + x + 2 \equiv 2x^4 + x^3 + 2x^2 + 2x(\text{mód } x^2 + 2)$$

pues $(2x^4 + x^3 + 2x^2 + 2x) - (x^4 + 2x^3 + x^2 + x + 2) = (x^2 + 2)(x^2 + 2x + 2)$.

$$x^4 + x^3 + 2x^2 + 1 \not\equiv x^3 + x + 2(\text{mód } x^2 + 2)$$

ya que $(x^3 + x + 2) - (x^4 + x^3 + 2x^2 + 1) = 2x^2(x^2 + 2) + (x + 1)$.

Proposición 3.4.1. *Sea $m(x) \in K[x]$. Entonces la relación de congruencia módulo $m(x)$ es una relación de equivalencia.*

La demostración es igual a la que se hizo para congruencias en $\mathbb{Z}$.

Para cada $m(x) \in K[x]$ vamos a denotar por $K[x]_{m(x)}$ al conjunto cociente de $K[x]$ por la relación de congruencia módulo $m(x)$. A la clase de equivalencia de un polinomio $a(x)$ la denotaremos inicialmente por $[a(x)]_{m(x)}$, o simplemente $[a(x)]$.

Al igual que en el caso de los números enteros, se tiene que $a(x) \equiv b(x)(\text{mód } m(x))$ si, y sólo si, $a(x)$ mód $m(x) = b(x)$ mód $m(x)$ (es decir, dan el mismo resto al dividir por $m(x)$). A partir de aquí puede verse que el conjunto $K[x]_{m(x)}$ está en biyección con los polinomios de $K[x]$ de grado menor que el de $m(x)$, pues hay tantos elementos como posibles restos de la división por $m(x)$.

Ejemplo 3.4.2.

1. *Vamos a calcular los elementos del conjunto* $\mathbb{Z}_2[x]_{(x^2+1)}$.

   Sea $p(x) \in \mathbb{Z}_2[x]$. *Si dividimos* $p(x)$ *entre* x^2+1, *sólo tenemos cuatro posibles restos, que son* 0, 1, x *y* $x+1$, *ya que el resto es de grado menor que* 2. *Tenemos entonces que*

   $$\mathbb{Z}_2[x]_{x^2+1} = \{[0], [1], [x], [x+1]\}.$$

   En la clase de equivalencia $[0]$ *están todos los polinomios que dan resto cero al dividir por* x^2+1, *es decir, todos los múltiplos de* x^2+1, *por ejemplo,* 0, x^2+1, x^3+x, x^4+1, *etc.; en la clase* $[1]$ *están los polinomios que al dividir por* x^2+1 *dan resto* 1, *como por ejemplo,* 1, x^2, x^3+x+1, x^4, *etc.*

   En resumen, se tiene:

   $$[0] = \{0,\ x^2+1,\ x^3+x,\ x^3+x^2+x+1,\ x^4+x^2,\ x^4+1, x^4+x^3+x^2+x,\ x^4+x^3+x+1, \cdots\}.$$
   $$[1] = \{1,\ x^2,\ x^3+x+1,\ x^3+x^2+x,\ x^4+x^2+1,\ x^4,\ x^4+x^3+x^2+x+1,\ x^4+x^3+x, \cdots\}.$$
   $$[x] = \{x,\ x^2+x+1,\ x^3,\ x^3+x^2+1,\ x^4+x^2+x,\ x^4+x+1,\ x^4+x^3+x^2,\ x^4+x^3+1, \cdots\}.$$
   $$[x+1] = \{x+1,\ x^2+x,\ x^3+1,\ x^3+x^2,\ x^4+x^2+x+1,\ x^4+x,\ x^4+x^3+x^2+1,\ x^4+x^3, \cdots\}.$$

   O si queremos,

   $$[0] = (x^2+1)\mathbb{Z}_2[x]; \qquad [1] = 1 + (x^2+1)\mathbb{Z}_2[x];$$
   $$(x] = x + (x^2+1)\mathbb{Z}_2[x]; \qquad [x+1] = x + 1 + (x^2+1)\mathbb{Z}_2[x].$$

   Y por ejemplo, se tiene que $x^8+x^7+x^6+x+1 \in [1]$, *ya que*

   $$x^8+x^7+x^6+x+1 = 1 + (x^2+1)\cdot(x^6+x^5+x^3+x).$$

2. *El conjunto* $\mathbb{Z}_2[x]_{x^2+x+1}$ *tiene también cuatro elementos, que son* $[0]$, $[1]$, $[x]$ *y* $[x+1]$. *Sin embargo, aunque se representen igual que los de* $\mathbb{Z}_2[x]_{x^2+1}$, *los conjuntos* $\mathbb{Z}_2[x]_{x^2+x+1}$ *y* $\mathbb{Z}_2[x]_{x^2+1}$ *son distintos, pues en cada uno* $[0]$, $[1]$, $[x]$ *y* $[x+1]$ *representa cosas diferentes. Veámoslo.*

   $$[0] = \{0,\ x^2+x+1,\ x^3+x^2+x,\ x^3+1,\ x^4+x^3+x^2,\ x^4+x^3+x+1,\ x^4+x,\ x^4+x^2+1, \cdots\}.$$
   $$[1] = \{1,\ x^2+x,\ x^3+x^2+x+1,\ x^3,\ x^4+x^3+x^2+1,\ x^4+x^3+x,\ x^4+x+1,\ x^4+x^2, \cdots\}.$$
   $$[x] = \{0,\ x^2+1,\ x^3+x^2,\ x^3+x+1,\ x^4+x^3+x^2+x,\ x^4+x^3+1,\ x^4,\ x^4+x^2+x+1, \cdots\}.$$
   $$[x+1] = \{0,\ x^2,\ x^3+x^2+1,\ x^3+x,\ x^4+x^3+x^2+x+1,\ x^4+x^3,\ x^4+1,\ x^4+x^2+x, \cdots\}.$$

   Y vemos como, por ejemplo, en el primer caso, es decir, $\mathbb{Z}_2[x]_{x^2+1}$ *se tiene que* $x^3 \in [x]$ *(o* $[x^3] = [x]$*), mientras que en el segundo caso, es decir,* $\mathbb{Z}_2[x]_{x^2+x+1}$ *se tiene que* $x^3 \in [1]$.

3. *El conjunto* $\mathbb{Z}_2[x]_{x^3+x^2+x+1}$ *tiene ocho elementos, mientras que* $\mathbb{Z}_3[x]_{x^2+1}$ *tiene nueve. Determínalos en ambos casos.*

Lema 3.4.1. *Sean* $a(x), b(x), c(x), d(x), m(x) \in K[x]$. *Entonces:*

1. $\left.\begin{array}{l} a(x) \equiv c(x) (mód\ m(x)) \\ b(x) \equiv d(x) (mód\ m(x)) \end{array}\right\} \Longrightarrow a(x)+b(x) \equiv c(x)+d(x) (mód\ m(x)).$

2. $\left.\begin{array}{l} a(x) \equiv c(x) (mód\ m(x)) \\ b(x) \equiv d(x) (mód\ m(x)) \end{array}\right\} \Longrightarrow a(x)b(x) \equiv c(x)d(x) (mód\ m(x)).$

Y con este lema podemos ya definir las operaciones suma y producto

Definición 53. *Sean* $a(x), b(x) \in K[x]$ *y* $m(x) \in K[x]$ *mónico y no constante. Se definen en* $K[x]_{m(x)}$ *las operaciones:*

$$[a(x)] + [b(x)] = [a(x)+b(x)], \qquad [a(x)][b(x)] = [a(x)b(x)].$$

Como era de esperar, la definición hecha no depende de los representantes elegidos.

Ejemplo 3.4.3.

1. *Supongamos que estamos trabajando en* $\mathbb{Z}_3[x]_{x^2+1}$.

   $[x+2]+[x+1]=[2x]$.

   $[x+2][x+1]=[x^2+2]=[1]$.

   Puesto que $[x+2]=[x^2+x]$ *y* $[x+1]=[2x^2+x]$ *podíamos haber efectuado las operaciones anteriores*

   $[x^2+x]+[2x^2+x]=[3x^2+2x]=[2x]$.

   $[x^2+x][2x^2+x]=[2x^4+x^2]=[1]$, *ya que* $2x^4+x^2=(x^2+1)(2x^2+2)+1$.

   Y los resultados coinciden, como no podía ser de otra forma.

2. *Vamos a fijarnos ahora en las clases de equivalencia que hemos obtenido en el ejemplo 3.4.2. En ese ejemplo, calculamos las clases de equivalencia que determinanban el conjunto* $\mathbb{Z}_2[x]_{x^2+1}$ *y las que determinaban el conjunto* $\mathbb{Z}_2[x]_{x^2+x+1}$.

   Vamos a sumar un elemento cualquiera de $[1]$ *con un elemento cualquiera de* $[x]$. *El resultado va a ser un elemento de* $[x+1]$. *Lo vamos a hacer cuatro veces.*

   - *Primero lo vamos a hacer con clases de* $\mathbb{Z}_2[x]_{x^2+1}$.

     $1+x=x+1\in[x+1]$ $\qquad$ $(x^3+x^2+x)+(x^2+x+1)=x^3+1\in[x+1]$

     $x^2+(x^4+x^3+x^2)=x^4+x^3\in[x+1]$ $\qquad$ $(x^4+x^3+x)+(x^4+x^3+x^2)=x^2+x\in[x+1]$.

     Y así para cualesquiera dos polinomios que tomemos, el primero perteneciente a $[1]$ *y el segundo a* $[x]$.

   - *Ahora lo hacemos en* $\mathbb{Z}_2[x]_{x^2+x+1}$.

     $(x^2+x)+(x^2+1)=x+1\in[x+1]$ $\qquad$ $x^3+(x^4+x^3+1)=x^4+1\in[x+1]$

     $(x^4+x^3+x)+(x^3+x+1)=x^4+1\in[x+1]$ $\qquad$ $(x^4+x^2)+x^4=x^2\in[x+1]$.

De ahora en adelante, si $a\in K\subseteq K[x]$, denotaremos por a a la clase de equivalencia $[a]\in K[x]_{m(x)}$, mientras que denotaremos por α a la clase de equivalencia $[x]$ (aunque es también frecuente representar por x a $[x]$).

Nótese que siguiendo esta notación, dado $a_kx^k+\cdots+a_1x+a_0\in K[x]$ el elemento $[a_kx^k+\cdots+a_1x+a_0]$ se representa como $a_k\alpha^k+\cdots+a_1\alpha+a_0$. Dicho de otra forma, $[p(x)]$ se representa como $p(\alpha)$.

Nótese también que con esta notación se verifica que $m(\alpha)=0$, pues $m(\alpha)=[m(x)]=[0]$. Además, esta condición es suficiente para realizar las operaciones en $K[x]_{m(x)}$

$$K[x]_{m(x)}=\{p(\alpha):p(x)\in K[x];m(\alpha)=0\}.$$

Al igual que ocurría con los conjuntos $\mathbb{Z}_m$, en los conjuntos que hemos construído, $K[x]_{m(x)}$, también tenemos definidas las operaciones suma y producto. El lema 3.4.1 nos asegura que estas definiciones son correctas.

Ejemplo 3.4.4.

1. *En el conjunto* $\mathbb{Z}_2[x]_{x^3+x+1}$ *vamos a multiplicar* $[x^2+x+1]$ *y* $[x^2+1]$. *Podemos proceder de dos formas:*

   a) *Multiplicamos los dos polinomios:*

   $[x^2+x+1][x^2+1]=[x^4+x^3+x+1]$.

   Dividimos x^4+x^3+x+1 *entre* x^3+x+1. $x^4+x^3+x+1=(x^3+x+1)(x+1)+x^2+x$.

   Por tanto $[x^2+x+1][x^2+1]=[x^2+x]$.

b) $(\alpha^2+\alpha+1)(\alpha^2+1)=\alpha^4+\alpha^3+\alpha+1$.
Puesto que $\alpha^3+\alpha+1=0$ *deducimos que* $\alpha^3=\alpha+1$, *luego* $\alpha^4=\alpha^2+\alpha$. *Por tanto* $(\alpha^2+\alpha+1)(\alpha^2+1)=\alpha^4+\alpha^3+\alpha+1=(\alpha^2+\alpha)+(\alpha+1)+\alpha+1=\alpha^2+\alpha$.

En los dos casos se obtiene el mismo resultado.

2. $\mathbb{Z}_2[x]_{x^2+1}=\{0,1,\alpha,\alpha+1:\alpha^2+1=0\}$, *o si preferimos:*

$$\mathbb{Z}_2[x]_{x^2+1}=\{0,1,\alpha,\alpha+1:\alpha^2=1\}.$$

Proposición 3.4.2. *Sea* $m(x)\in k[x]$ *mónico y no constante. Las operaciones suma y producto en* $K[x]_{m(x)}$ *verifican las siguientes propiedades:*

i) $p(\alpha)+(q(\alpha)+r(\alpha))=(p(\alpha)+q(\alpha))+r(\alpha)$

ii) $p(\alpha)+q(\alpha)=q(\alpha)+p(\alpha)$

iii) $p(\alpha)+0=p(\alpha)$

iv) Para cada $p(\alpha)\in K[x]_{m(x)}$ *existe* $q(\alpha)\in K[x]_{m(x)}$ *tal que* $p(\alpha)+q(\alpha)=0$.

v) $p(\alpha)(q(\alpha)r(\alpha))=(p(\alpha)q(\alpha))r(\alpha)$

vi) $p(\alpha)q(\alpha)=q(\alpha)p(\alpha)$

vii) $p(\alpha)1=p(\alpha)$

viii) $p(\alpha)(q(\alpha)+r(\alpha))=p(\alpha)q(\alpha)+p(\alpha)r(\alpha)$

Estas propiedades nos dicen que $K[x]_{m(x)}$ es un anillo conmutativo.

Ejemplo 3.4.5.

1. *Consideramos el anillo* $\mathbb{Z}_2[x]_{x^3+1}$. *Vamos a escribir las tablas de sumar y multiplicar de dicho anillo. Antes de ello, enumeramos sus elementos*

$$\mathbb{Z}_2[x]_{x^3+1}=\{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$$

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

Para realizar la tabla del producto tenemos en cuenta que $\alpha^3+1=0$, *es decir,* $\alpha^3=1$.

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	1	$\alpha+1$	α^2+1	$\alpha^2+\alpha+1$
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2+1	$\alpha^2+\alpha$	$\alpha+1$	0
α^2	0	α^2	1	α^2+1	α	$\alpha^2+\alpha$	$\alpha+1$	$\alpha^2+\alpha+1$
α^2+1	0	α^2+1	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha+1$	α^2+1	0
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	α^2+1	$\alpha+1$	$\alpha+1$	α^2+1	$\alpha^2+\alpha$	0
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	0	0	$\alpha^2+\alpha+1$

Donde algunas de las celdas se han completado como sigue:

$$\alpha \cdot \alpha^2 = \alpha^3 = 1$$

$$(\alpha^2+1)(\alpha^2+\alpha+1) = \alpha^4+\alpha^3+\alpha^2+\alpha^2+\alpha+1 = \alpha+1+\alpha^2+\alpha^2+\alpha+1 = 0$$

Y se ha tenido en cuenta que $\alpha^4 = \alpha^3 \cdot \alpha = \alpha$.

$$(\alpha^2+1)(\alpha^2+1) = \alpha^4+2\alpha^2+1 = \alpha+1.$$

2. *Vamos a dar ahora la tabla de multiplicar de* $\mathbb{Z}_3[x]_{x^2+1}$. *Los elementos son ahora*

$$\mathbb{Z}_3[x]_{x^2+1} = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$$

$\cdot$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	2	$\alpha+2$	$2\alpha+2$	1	$\alpha+1$	$2\alpha+1$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$\alpha+2$	2α	1	$2\alpha+1$	2	α
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	1	α	$\alpha+1$	2α	2
2α	0	2α	α	1	$2\alpha+1$	$\alpha+1$	2	$2\alpha+2$	$\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$\alpha+1$	2	2α	$2\alpha+2$	α	1
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$2\alpha+1$	α	2	$\alpha+2$	1	2α

Definición 54. *Sea* A *un anillo conmutativo.*

- *Se dice que* $a \in A$ *es una unidad si existe* $b \in A$ *tal que* $ab = 1$. *En tal caso, se dice que* b *es el inverso de* a, *y escribiremos* $b = a^{-1}$.
- *Se dice que* $a \in A$ *es un divisor de cero si existe* $b \in A$, $b \neq 0$ *tal que* $ab = 0$.

Un anillo conmutativo en el que 0 *es el único divisor de cero se llama* dominio de integridad.
Un anillo conmutativo en el que todo elemento no nulo es una unidad es un cuerpo.

Ejemplo 3.4.6.

1. *En cualquier anillo,* 1 *es una unidad, pues* $1 \cdot 1 = 1$, *mientras que* 0 *es un divisor de cero, pues* $0 \cdot 1 = 0$.
2. *En* $\mathbb{Z}_2[x]_{x^3+1}$ *son divisores de cero:*

$$0 \qquad \alpha+1 \qquad \alpha^2+1 \qquad \alpha^2+\alpha \qquad \alpha^2+\alpha+1$$

mientras que son unidades:

$$1 \qquad \alpha \qquad \alpha^2$$

como puede comprobarse a partir del ejemplo anterior.

3. *En* $\mathbb{Z}_3[x]_{x^2+1}$, *el único divisor de cero es* 0. *Todos los demás elementos son unidades.*
4. *En* $\mathbb{Z}$, *las unidades son* 1 *y* -1. *El único divisor de cero es* 0.
5. *Todo cuerpo es un dominio de integridad. El recíproco no es cierto, pues* $\mathbb{Z}$ *es un dominio de integridad pero no es un cuerpo.*

Proposición 3.4.3. *Sea K un cuerpo, $m(x) \in K[x]$ no constante y $p(\alpha) \in K[x]_{m(x)}$. Entonces:*

- *$p(\alpha)$ es una unidad si, y sólo si, $mcd(p(x), m(x)) = 1$.*
- *$p(\alpha)$ es un divisor de cero si, y sólo si, $mcd(p(x), m(x)) \neq 1$.*

Demostración: La demostración de la primera parte es análoga a la demostración de la proposición 2.6.2

En cuanto a la segunda, si $p(\alpha)$ es un divisor de cero, entonces $p(\alpha)$ no es una unidad (¿por qué?), luego $mcd(p(x), m(x)) \neq 1$.

Recíprocamente, si $mcd(p(x), m(x)) \neq 1$, consideramos $q(x) = \frac{m(x)}{d(x)}$ donde $d(x) = mcd(p(x), m(x))$. Entonces $gr(q(x)) < gr(m(x))$, lo que implica que $q(\alpha) \neq 0$, y puesto que $p(x)q(x)$ es múltiplo de $m(x)$ ya que

$$p(x)q(x) = p(x)\frac{m(x)}{d(x)} = \frac{p(x)}{d(x)}m(x)$$

se verifica que $p(\alpha)q(\alpha) = 0$. ■

Ejemplo 3.4.7. *En $\mathbb{Z}_2[x]$ se verifica que $mcd(x^2+1, x^3+1) = x+1$. Por tanto, α^2+1 es un divisor de cero en $\mathbb{Z}_2[x]_{x^3+1}$. Además, para encontrar un elemento que al multiplicarlo por él nos de cero, calculamos $\frac{x^3+1}{x+1}$. Ese cociente vale x^2+x+1. Deducimos entonces que $(\alpha^2+1)(\alpha^2+\alpha+1) = 0$, como podemos ver en el ejemplo anterior.*

A partir de la proposición anterior se deduce fácilmente que si $m(x)$ es un polinomio irreducible en $K[x]$, entonces $K[x]_{m(x)}$ es un cuerpo. Si $m(x)$ es un polinomio irreducible de grado n en $\mathbb{Z}_p[x]$ entonces $\mathbb{Z}_p[x]_{m(x)}$ es un cuerpo con p^n elementos.

Por otra parte, si K es un cuerpo con un número finito de elementos, entonces su característica es un número primo p (la característica de un anillo A se define como el menor número natural m tal que $1 + 1 + \overset{m \text{ veces}}{\cdots} + 1 = 0$, si dicho número existe). En tal caso se tiene que $\mathbb{Z}_p \subseteq K$. Utilizando resultados de álgebra lineal se tiene que existe un número natural n tal que K tiene p^n elementos.

Es decir, por una parte hemos visto que el número de elementos de un cuerpo finito es una potencia de un primo. Por otra parte, hemos visto como, dado un número primo p y un número natural n podemos construir un cuerpo con p^n elementos. Basta encontrar un polinomio irreducible de grado n en $\mathbb{Z}_p[x]$. Hay un teorema que nos asegura la existencia de polinomios irreducibles de cualquier grado en $\mathbb{Z}_p[x]$.

La existencia de varios polinomios irreducibles de un mismo grado en $\mathbb{Z}_p[x]$ daría lugar, en principio, a distintos cuerpos con p^n elementos. Sin embargo, todos los cuerpos con el mismo cardinal son isomorfos, en el sentido que vamos a explicar a continuación.

Ejemplo 3.4.8.

1. *Hemos visto que $\mathbb{Z}_3[x]_{x^2+1}$ es un cuerpo con nueve elementos, cuya tabla del producto calculamos en el ejemplo 3.4.5. Puesto que x^2+x+2 es también un polinomio irreducible en $\mathbb{Z}_3[x]$ tenemos que $\mathbb{Z}_3[x]_{x^2+x+2}$ es también un cuerpo con nueve elementos. Si llamamos β al elemento $[x]$, entonces la tabla del producto de este cuerpo es:*

$(\mathbb{Z}_3[x]_{x^2+x+2}, \cdot)$	0	1	2	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$
2	0	2	1	2β	$2\beta+2$	$2\beta+1$	β	$\beta+2$	$\beta+1$
β	0	β	2β	$2\beta+1$	1	$\beta+1$	$\beta+2$	$2\beta+2$	2
$\beta+1$	0	$\beta+1$	$2\beta+2$	1	$\beta+2$	2β	2	β	$2\beta+1$
$\beta+2$	0	$\beta+2$	$2\beta+1$	$\beta+1$	2β	2	$2\beta+2$	1	β
2β	0	2β	β	$\beta+2$	2	$2\beta+2$	$2\beta+1$	$\beta+1$	1
$2\beta+1$	0	$2\beta+1$	$\beta+2$	$2\beta+2$	β	1	$\beta+1$	2	2β
$2\beta+2$	0	$2\beta+2$	$\beta+1$	2	$2\beta+1$	β	1	2β	$\beta+2$

donde se ha usado que $\beta^2 = 2\beta + 1$, relación que se deduce de $\beta^2 + \beta + 2 = 0$ (es decir, $m(\beta) = 0$).

Si ahora hacemos el cambio $\alpha = \beta + 2$, es decir, $\beta = \alpha + 1$, la tabla nos quedaría

$(\mathbb{Z}_3[x]_{x^2+x+2}, \cdot)$	0	1	2	$\alpha+1$	$\alpha+2$	α	$2\alpha+2$	2α	$2\alpha+1$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$\alpha+1$	$\alpha+2$	α	$2\alpha+2$	2α	$2\alpha+1$
2	0	2	1	$2\alpha+2$	$2\alpha+1$	2α	$\alpha+1$	α	$\alpha+2$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	2α	1	$\alpha+2$	α	$2\alpha+1$	2
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	1	α	$2\alpha+2$	2	$\alpha+1$	2α
α	0	α	2α	$\alpha+2$	$2\alpha+2$	2	$2\alpha+1$	1	$\alpha+1$
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	α	2	$2\alpha+1$	2α	$\alpha+2$	1
2α	0	2α	α	$2\alpha+1$	$\alpha+1$	1	$\alpha+2$	2	$2\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	2	2α	$\alpha+1$	1	$2\alpha+2$	α

Si comparamos esta tabla con la que obtuvimos para $\mathbb{Z}_3[x]_{x^2+1}$ vemos que es exactamente la misma (salvo el orden de las filas y columnas). Vemos entonces que los cuerpos $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_3[x]_{x^2+x+2}$ son iguales, o más precisamente, son isomorfos.

De hecho, lo único que diferencia a los cuerpos $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_3[x]_{x^2+x+2}$ es, aparte del camino para obtenerlos, el nombre que se le ha dado a los elementos. Lo que en un cuerpo se llama α en el otro se llama $\beta + 2$. Una vez hecha la correcta correspondencia entre los elementos de uno y del otro, se opera de igual forma en un caso y en el otro.

Nota: *Dados dos cuerpos K y K', se dice que son isomorfos si existe una aplicación $f : K \to K'$ satisfaciendo:*

a) *f preserva la suma, es decir, $f(a + b) = f(a) + f(b)$.*

b) *f preserva el producto, es decir, $f(ab) = f(a)f(b)$.*

c) *f es biyectiva.*

f es lo que se llama un isomorfismo de cuerpos.

En el caso de $K = \mathbb{Z}_3[x]_{x^2+x+2}$ y $K' = \mathbb{Z}_3[x]_{x^2+1}$, la aplicación $f : K \to K'$ dada por

$$0 \mapsto 0 \quad 1 \mapsto 1 \quad 2 \mapsto 2 \quad \beta \mapsto \alpha + 1 \quad \beta + 1 \mapsto \alpha + 2$$

$$\beta + 2 \mapsto \alpha \quad 2\beta \mapsto 2\alpha + 2 \quad 2\beta + 1 \mapsto 2\alpha \quad 2\beta + 2 \mapsto 2\alpha + 1$$

es un isomorfismo de cuerpos. Obviamente, este isomorfismo queda totalmente determinado por $\beta \mapsto \alpha + 1$.

2. *Nos situamos en el cuerpo de los números reales. Entonces el polinomio $x^2 + 1$ es irreducible, luego $\mathbb{R}[x]_{x^2+1}$ es un cuerpo. Si llamamos i al elemento $[x]$, entonces se tiene que los elementos de $\mathbb{R}[x]_{x^2+1}$ son de la forma $a + bi$, donde $a, b \in \mathbb{R}$. Además, $i^2 + 1 = 0$, es decir, $i^2 = -1$.*

   Por tanto,

$$\mathbb{R}[x]_{x^2+1} = \{a + bi : a, b \in \mathbb{R}; i^2 = -1\}$$

   luego el cuerpo obtenido resulta ser igual (o isomorfo) a $\mathbb{C}$.

Dado p es un número primo y n es un número natural no nulo, denotaremos como $\mathbb{F}_{p^n}$ al único cuerpo que existe con p^n elementos. Así, por ejemplo, $\mathbb{F}_4 = \mathbb{Z}_2[x]_{x^2+x+1}$ y $\mathbb{F}_9 = \mathbb{Z}_3[x]_{x^2+1}$. Obviamente, $\mathbb{F}_p = \mathbb{Z}_p$ para cualquier primo p.

3.5. Sistemas de congruencias de polinomios

Al igual que se hizo con los números enteros, nos planteamos encontrar todos los polinomios $p(x) \in K[x]$ que verifican la relación

$$a(x)p(x) \equiv b(x)(\text{mód } m(x))$$

con $a(x), b(x), m(x) \in K[x]$.

Un polinomio $q(x) \in K[x]$ para el que se verifique que $a(x)q(x) \equiv b(x)(\text{mód } m(x))$ es una solución de la congruencia.

Dos congruencias de la forma $a_1(x)p(x) \equiv b_1(x)(\text{mód } m_1(x))$ y $a_2(x)p(x) \equiv b_2(x)(\text{mód } m_2(x))$ son equivalentes si toda solución de la primera es solución de la segunda y viceversa.

La forma de resolver estas congruencias es análoga a la que seguíamos para resolverlas en $\mathbb{Z}$. Transformamos (si es posible) la congruencia $a(x)p(x) \equiv b(x)(\text{mód } m(x))$ en otra equivalente de la forma $p(x) \equiv c(x)(\text{mód } n(x))$, cuyas soluciones son

$$p(x) = c(x) + q(x)n(x) : \quad q(x) \in K[x]$$

Los resultados necesarios para resolver estas congruencias son:

1. Si $a_1(x) \equiv a_2(x)(\text{mód } m(x))$ y $b_1(x) \equiv b_2(x)(\text{mód } m(x))$ entonces las congruencias $a_1(x)p(x) \equiv b_1(x)(\text{mód } m(x))$ y $a_2(x)p(x) \equiv b_2(x)(\text{mód } m(x))$ son equivalentes.
2. Si $d(x)$ es un divisor común de $a(x)$, $b(x)$ y $m(x)$, las congruencias

   $$a(x)p(x) \equiv b(x)(\text{mód } m(x)) \qquad \frac{a(x)}{d(x)}p(x) \equiv \frac{b(x)}{d(x)}(\text{mód } \frac{m(x)}{d(x)})$$

   son equivalentes.
3. Si $mcd(m(x), c(x)) = 1$ entonces las congruencias

   $$a(x)p(x) \equiv b(x)(\text{mód } m(x)) \qquad c(x)a(x)p(x) \equiv c(x)b(x)(\text{mód } m(x))$$

   son equivalentes.

Proposición 3.5.1. *Sea K un cuerpo, y $a(x), b(x), m(x) \in K[x]$ tales que $gr(m(x)) \geq 1$. Entonces*

$$a(x)p(x) \equiv b(x)(\textit{mód } m(x))$$

tiene solución si, y sólo si, $mcd(a(x), m(x))|b(x)$.

Para resolver congruencias de la forma $a(x)p(x) \equiv b(x)(\text{mód } m(x))$ podemos proceder como sigue:

- Reducimos $a(x)$ y $b(x)$ módulo $m(x)$.
- Se comprueba si $mcd(a(x), m(x))|b(x)$. Si la respuesta es negativa, entonces la congruencia no tiene solución. Si la respuesta es afirmativa, podemos dividir toda la congruencia por $mcd(a(x), m(x))$.

  Hemos transformado la congruencia en una de la forma $a(x)p(x) \equiv b(x)(\text{mód } m(x))$, pero ahora se tiene que $mcd(a(x), m(x)) = 1$.
- Buscamos el inverso de $[a(x)]$ en $K[x]_{m(x)}$. Supongamos que es $[u(x)]$.
- Multiplicamos ambos miembros de la congruencia por $u(x)$. Obtenemos así una congruencia equivalente, y ésta adopta la forma $p(x) \equiv c(x)(\text{mód } m(x))$.

Con esto ya hemos resuelto la congruencia. Las soluciones son $p(x) = c(x) + q(x)m(x) : \ q(x) \in K[x]$.

Ejemplo 3.5.1. *Vamos a resolver en* $\mathbb{Z}_{11}[x]$ *la congruencia*

$$(x^2+6x+9)p(x) \equiv 3x^3+7x^2+9x+2(mód\ x^3+5x^2+10x+3)$$

Reducimos módulo $x^3+5x^2+10x+2$.

$$(x^2+6x+9)p(x) \equiv 3x^2+x+4(mód\ x^3+5x^2+10x+3).$$

Hallamos el máximo común divisor de x^2+6x+9 *y* $x^3+5x^2+10x+3$.

$p(x)$	$q(x)$	a
$x^3+5x^2+10x+3$	x^2+6x+9	
x^2+6x+9	$7x+1$	
$7x+1$	3	
3	0	4
1		

Puesto que este máximo común divisor vale 1 *hallamos el inverso de* x^2+6x+9 *módulo* $x^3+5x^2+10x+3$.

a	$r(x)$	$c(x)$	$v(x)$
	$x^3+5x^2+10x+3$		0
	x^2+6x+9		1
	$7x+1$	$x+10$	$10x+1$
	3	$8x+6$	$8x^2+9x+6$
4	0		
	1		$\mathbf{10x^2+3x+2}$

Multiplicamos por $10x^2+3x+2$.

$$(10x^4+8x^3+6x+7)p(x) \equiv 8x^4+8x^3+5x^2+3x+8(mód\ x^3+5x^2+10x+3).$$

Reducimos módulo $x^3+5x^2+10x+3$.

$$p(x) \equiv 8x^2+2x+5(mód\ x^3+5x^2+10x+3).$$

Luego la solución es

$$p(x) = 8x^2+2x+5+c(x)(x^3+5x^2+10x+3): \quad c(x) \in \mathbb{Z}_{11}[x].$$

En lo referente a un sistema de congruencias se tiene también el teorema chino del resto.

Teorema 3.5.1. *Sean* $a_1(x), \cdots, a_k(x) \in K[x]$ *y sean* $m_1(x), \cdots, m_k(x) \in K[x]$ *tales que* $mcd(m_i(x), m_j(x)) = 1$. *Entonces el sistema*

$$\begin{gathered} p(x) \equiv a_1(x)(mód\ m_1(x)) \\ p(x) \equiv a_2(x)(mód\ m_2(x)) \\ \cdots\cdots\cdots\cdots \\ p(x) \equiv a_k(x)(mód\ m_k(x)) \end{gathered}$$

tiene solución. Además, si $a(x)$ *es una solución, el sistema es equivalente a la congruencia*

$$p(x) \equiv a(x)(mód\ M(x))$$

donde $M(x) = \prod_{i=1}^{k} m_i(x)$.

Sin embargo, a la hora de resolver sistemas de congruencias, procederemos a resolverlo progresivamente. Resolvemos la primera congruencia; introducimos esta solución en la segunda congruencia y la resolvemos; y así sucesivamente. De esta forma, no estamos sujetos a que se satisfagan las hipótesis del teorema chino. Veamos un ejemplo.

Ejemplo 3.5.2. *Vamos a resolver el sistema de congruencias en* $\mathbb{Z}_5[x]$.

$$\begin{array}{c} p(x) \equiv x+2(mód\ x^2+1) \\ (x+1)p(x) \equiv x^2+1(mód\ x^3+2x^2+2) \\ x^2p(x) \equiv 3x+2(mód\ x^2+x+1) \end{array}$$

Resolvemos la primera congruencia:

$$p(x) = x+2+(x^2+1)q_1(x).$$

Introducimos esta solución en la segunda congruencia.

$$\begin{aligned} &(x+1)(x+2+(x^2+1)q_1(x)) \equiv x^2+1(mód\ x^3+2x^2+2); \\ &x^2+3x+2+(x^3+x^2+x+1)q_1(x) \equiv x^2+1(mód\ x^3+2x^2+2); \\ &(x^3+x^2+x+1)q_1(x) \equiv 2x+4(mód\ x^3+2x^2+2); \\ &(4x^2+x+4)q_1(x) \equiv 2x+4(mód\ x^3+2x^2+2). \end{aligned}$$

A continuación calculamos el inverso de $4x^2+x+4$ *módulo* x^3+2x^2+2.

a	$r(x)$	$c(x)$	$v(x)$
	x^3+2x^2+2		0
	$4x^2+x+4$		1
	$2x+4$	$4x+2$	$x+3$
	3	$2x+4$	$3x^2+4$
2	0		
	$\mathbf{1}$		$\mathbf{x^2+3}$

Multiplicamos entonces por x^2+3.

$$\begin{aligned} &q_1(x) \equiv (x^2+3)(2x+4)(mód\ x^3+2x^2+2); \\ &q_1(x) \equiv 2x^3+4x^2+x+2(mód\ x^3+2x^2+2); \\ &q_1(x) \equiv x+3(mód\ x^3+2x^2+2). \end{aligned}$$

Luego $q_1(x) = x+3+q_2(x)(x^3+2x^2+2)$ *y por tanto* $p(x) = x^3+3x^2+2x+q_2(x)(x^5+2x^4+x^3+4x^2+2)$ *Introducimos esta solución en la tercera congruencia, y operamos:*

$$\begin{aligned} &x^2(x^3+3x^2+2x)+x^2(x^5+2x^4+x^3+4x^2+2)q_2(x) \equiv 3x+2(mód\ x^2+x+1); \\ &(x^7+2x^6+x^5+4x^4+2x^2)q_2(x) \equiv 4x^5+2x^4+3x^3+3x+2(mód\ x^2+x+1); \\ &(2x+4)q_2(x) \equiv x+1(mód\ x^2+x+1). \end{aligned}$$

Calculamos el inverso de $2x+4$ *módulo* x^2+x+1, *y resulta ser* $4x+1$. *Multiplicamos entonces por este polinomio.*

$$\begin{aligned} &q_2(x) \equiv (x+1)(4x+1)(mód\ x^2+x+1); \\ &q_2(x) \equiv 4x^2+1(mód\ x^2+x+1); \\ &q_2(x) \equiv x+2(mód\ x^2+x+1). \end{aligned}$$

Por tanto, se tiene que $q_2(x) = x+2+q(x)(x^2+x+1)$. *Introducimos este valor en lo que ya teníamos para* $p(x)$ *y nos queda:*

$$p(x) = x^3+3x^2+2x+[x+2+(x^2+x+1)q(x)](x^5+2x^4+x^3+4x^2+2),$$

es decir:

$$p(x) = x^6 + 4x^5 + 2 * x^3 + x^2 + 4x + 1 + (x^7 + 3x^6 + 4x^5 + 2x^4 + x^2 + 2x + 2)q(x).$$

Un caso particularmente interesante es cuando queremos resolver un sistema de congruencias donde todos los módulos son polinomios mónicos (de la forma $x - a$). Para resolver este tipo de sistemas de congruencias es importante tener en cuenta que se verifica que

$$q(x) \equiv q(a)(\text{mód } x - a)$$

luego, para reducir un polinomio módulo $x - a$ basta con evaluar el polinomio en $x = a$.

Por otra parte, el inverso de $q(x)$ módulo $x - a$ es $q(a)^{-1}$ (este último calculado en K).

Por último, el problema de encontrar un polinomio $p(x)$ que satisfaga la congruencia $p(x) \equiv b(\text{mód } x - a)$ es equivalente al problema de encontrar un polinomio $p(x)$ que verifique que $p(a) = b$.

Nos planteamos entonces el siguiente problema:

> Dados $a_0, a_1, \cdots, a_m \in K$ todos distintos, y $b_0, b_1, \cdots, b_m \in K$, encontrar un polinomio $p(x) \in K[x]$ tal que $p(a_i) = b_i$.

Este problema se conoce como *problema de interpolación* y un polinomio solución se dice que es un polinomio interpolador.

Para resolverlo, planteamos el siguiente sistema de congruencias:

$$\begin{array}{c} p(x) \equiv b_0(\text{mód } x - a_0) \\ p(x) \equiv b_0(\text{mód } x - a_0) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ p(x) \equiv b_m(\text{mód } x - a_m) \end{array}$$

Cada una de las soluciones de este sistema será un polinomio interpolador.

Puesto que $mcd(x - a_i, x - a_j) = 1$ para $i \neq j$ deducimos, a partir del teorema chino, que este sistema tiene solución. Además, la solución es única módulo $\prod_{i=0}^{m}(x - a_i)$. Puesto que este polinomio tiene grado $m + 1$, deducimos que existe siempre un polinomio de grado menor o igual que m que interpola $m + 1$ datos.

Ejemplo 3.5.3. *Vamos a encontrar un polinomio en $\mathbb{Z}_7[x]$ que satisfaga que $p(1) = 2$, $p(2) = 5$, $p(4) = 6$ y $p(5) = 5$.*

Para ello, planteamos el sistema de congruencias

$$\begin{array}{c} p(x) \equiv 2(mód\ x + 6) \\ p(x) \equiv 5(mód\ x + 5) \\ p(x) \equiv 6(mód\ x + 3) \\ p(x) \equiv 5(mód\ x + 2) \end{array}$$

y procedemos a resolverlo como siempre:

Hallamos la solución de la primera congruencia

$$p(x) = 2 + (x + 6)q_1(x).$$

Introducimos esta solución en la segunda congruencia y operamos.

$$2 + (x + 6)q_1(x) \equiv 5(mód\ x + 5);$$
$$(x + 6)q_1(x) \equiv 3(mód\ x + 5);$$

$$q_1(x) \equiv 3(mód\ x+5);$$
$$q_1(x) = 3 + q_2(x)(x+5).$$

Luego resulta que $p(x) = 2 + (x+6)[3 + q_2(x)(x+5)] = 3x + 6 + (x+6)(x+5)q_2(x)$.
Continuamos introduciendo esta solución en la tercera congruencia.

$$3x + 6 + (x+6)(x+5)q_2(x) \equiv 6(mód\ x+3);$$
$$(x+6)(x+5)q_2(x) \equiv 4x(mód\ x+3);$$
$$6q_2(x) \equiv 2(mód\ x+3);$$
$$q_2(x) \equiv 5(mód\ x+3);$$
$$q_2(x) = 5 + q_3(x)(x+3).$$

Por tanto, $p(x) = 3x+6+(x+6)(x+5)[5+q_3(x)(x+3)] = 5x^2+2x+2+(x+6)(x+5)(x+3)q_3(x)$.

$$5x^2 + 2x + 2 + (x+6)(x+5)(x+3)q_3(x) \equiv 5(mód\ x+2);$$
$$(x+6)(x+5)(x+3)q_3(x) \equiv 2x^2 + 5x + 3(mód\ x+2);$$
$$5q_3(x) \equiv 1(mód\ x+2);$$
$$q_3(x) \equiv 3(mód\ x+2);$$
$$q_3(x) = 3 + q(x)(x+2).$$

Nos queda entonces que $p(x) = 5x^2 + 2x + 2 + (x+6)(x+5)(x+3)[3 + (x+2)q(x)]$, *es decir,*

$$p(x) = 3x^3 + 5x^2 + 2x + 6 + (x+6)(x+5)(x+3)(x+2)q(x),$$

luego una solución es $p(x) = 3x^3 + 5x^2 + 2x + 6$.

Basándonos en esta idea podemos diseñar un algoritmo que calcule un polinomio que interpole unos datos dados. Denominaremos a este algoritmo INTERPOLA

Algoritmo INTERPOLA$(m, a_0, b_0, a_1, b_1, \cdots, a_m, b_m)$
Entrada:
$m \in \mathbb{N}$
$a_0, b_0, a_1, b_1, \cdots, a_m, b_m \in K$
Salida: $p(x) \in K[x]$. $p(a_i) = b_i$ y $gr(p(x)) \leq n$
$p(x) := b_0$
$q(x) := x - a_0$
Desde $i = 1$ hasta m
$p(x) := p(x) + q(a_i)^{-1}(b_i - p(a_i)) \cdot q(x)$
$q(x) := q(x) \cdot (x - a_i)$
Devuelve $p(x)$
Fin

Veamos como resover el ejemplo anterior haciendo uso de este algoritmo.

i	a_i	b_i	$q(a_i)$	$q(a_i)^{-1}$	$p(a_i)$	$b_i - p(a_i)$	$p(x)$	$q(x)$
							2	$x+6$
1	2	5	1	1	2	3	$3x+6$	x^2+4x+2
2	4	6	6	6	4	2	$5x^2+2x+2$	x^3+6
3	5	5	5	3	4	1	$3x^3+5x^2+2x+6$	x^4+2x^3+6x+5

Luego el polinomio interpolador es $p(x) = 3x^3 + 5x^2 + 2x + 6$. Todos los polinomios que satisfacen las condiciones dadas adoptan la forma:

$$p(x) = 3x^3 + 5x^2 + 2x + 6 + c(x)(x^4 + 2x^3 + 6x + 5) : \quad c(x) \in \mathbb{Z}_7[x]$$

Vamos a comprobar que el polinomio $p(x)$ satisface las condiciones requeridas. Para ello, vamos a evaluarlo en $x = 1$, $x = 2$, $x = 4$ y $x = 5$.

	3	5	2	6
1		3	1	3
	3	1	3	**2**

	3	5	2	6
2		6	1	6
	3	4	3	**5**

	3	5	2	6
4		5	5	0
	3	3	0	**6**

	3	5	2	6
5		1	2	6
	3	6	4	**5**

$p(1) = 2$ $\quad$ $p(2) = 5$ $\quad$ $p(4) = 6$ $\quad$ $p(5) = 5$

Si nos fijamos en el algoritmo, vemos que lo que hacemos es expresar el polinomio interpolador como

$$p(x) = c_0 + c_1(x - a_0) + c_2(x - a_0)(x - a_1) + \cdots + c_n(x - a_0)(x - a_1) \cdots (x - a_{n-1})$$

Y el algoritmo nos calcula los coeficientes c_i. De hecho, se tiene que $c_i = q(a_i)^{-1}(b_i - p(a_i))$.

Estos coeficientes pueden calcularse también haciendo uso de las diferencias divididas. Vemos en que consiste.

Definición 55. *Sea K un cuerpo, y $f : K \to K$ una aplicación. Sean $a_0, a_1, \cdots, a_n \in K$ todos distintos. Se definen las diferencias divididas $f[a_i, a_{i+1}, \cdots, a_{i+k}]$ como sigue:*

$$f[a_i] = f(a_i)$$

$$f[a_i, a_{i+1}, \cdots, a_{i+k}] = \frac{f[a_{i+1}, \cdots, a_{i+k}] - f[a_i, \cdots a_{i+k-1}]}{a_{i+k} - a_i}$$

donde hemos usado la notación $\frac{a}{b}$ para representar $a \cdot b^{-1}$.

Ejemplo 3.5.4.

Sea $K = \mathbb{Z}_5$, sean $a_0 = 1$, $a_1 = 2$ y $a_2 = 4$, y sea $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ la aplicación dada por $f(x) = x^2 + 2x$. Entonces:

$f[a_0] = f(1) = 3$
$f[a_1] = f(2) = 3 \quad f[a_0, a_1] = \frac{f[a_1] - f[a_0]}{a_1 - a_0} = \frac{3-3}{2-1} = 0$
$f[a_2] = f(4) = 4 \quad f[a_1, a_2] = \frac{f[a_2] - f[a_1]}{a_2 - a_1} = \frac{4-3}{4-2} = 1 \cdot 3 = 3 \quad f[a_0, a_1, a_2] = \frac{f[a_1, a_2] - f[a_0, a_1]}{a_2 - a_0} = \frac{3-0}{4-1} = 1$

El interés de las diferencias divididas viene dado en el siguiente teorema.

Teorema 3.5.2. *Sea K un cuerpo, $a_0, a_1, \cdots, a_n \in K$ distintos, y $b_0, b_1, \cdots, b_n \in K$. Sea $p(x)$ el polinomio interpolador para estos datos, es decir, $p(x) \in K[x]$, $gr(p(x)) \leq n$ y $p(a_i) = b_i$. Entonces:*

$$p(x) = p[a_0] + p[a_0, a_1](x - a_0) + p[a_0, a_1, a_2](x - a_0)(x - a_1) + \cdots + p[a_0, a_1, \cdots, a_n](x - a_0)(x - a_1) \cdots (x - a_{n-1})$$

o en notación más compacta

$$p(x) = \sum_{i=0}^{n} p[a_0, \cdots a_i](x - a_0) \cdots (x - a_{i-1})$$

Ejemplo 3.5.5.

Vamos a calcular $p(x) \in \mathbb{Z}_5[x]$ que interpola a los datos $p(1) = 3$, $p(2) = 3$, $p(4) = 4$. Por el ejemplo 3.5.4 sabemos que ese polinomio es $p(x) = x^2 + 2x$.

Según el teorema que acabamos de ver, se tiene que

$$p(x) = p[1] + p[1, 2](x - 1) + p[1, 2, 4](x - 1)(x - 2) = 3 + 0(x - 1) + 1(x - 1)(x - 2) = 3 + x^2 - 3x + 2 = x^2 + 2x$$

El siguiente algoritmo nos calcula el polinomio interpolador haciendo uso de las diferencias divididas.

Algoritmo NEWTON$(m, a_0, b_0, a_1, b_1, \cdots, a_m, b_m)$
Entrada:
$m \in \mathbb{N}$
$a_0, b_0, a_1, b_1, \cdots, a_m, b_m \in K$
Salida: $p(x) \in K[x]$. $p(a_i) = b_i$ y $gr(p(x)) \leq m$
$p(x) := b_0$
$q(x) := (x - a_0)$
Desde $i = 1$ hasta m
Desde $j = m$ hasta i paso:(-1)
$b_j := \frac{b_j - b_{j-1}}{a_j - a_{j-i}}$
$p(x) := p(x) + b_i \cdot q(x)$
$q(x) := q(x) \cdot (x - a_i)$
Devuelve $p(x)$
Fin

Ejemplo 3.5.6.

Vamos a calcular $p(x) \in \mathbb{Z}_7[x]$ tal que $p(1) = 2$, $p(2) = 5$, $p(4) = 6$ y $p(5) = 5$. Es decir, el mismo polinomio que obtuvimos en el ejemplo 3.5.3.

Los cálculos que vayamos haciendo los vamos a representar en una tabla.

Comenzamos inicializando las variables.

		$i=0$					
	a_j	b_j				$p(x)$	$q(x)$
$j=0$	1	2				2	$x+6$
$j=1$	2	5					
$j=2$	4	6					
$j=3$	5	5					

Y ahora entramos en el bucle, con $i = 1$. Calculamos

$b_3 = \frac{b_3 - b_2}{a_3 - a_2} = \frac{5-6}{5-4} = (-1) \cdot 1^{-1} = 6$.
$b_2 = \frac{b_2 - b_1}{a_2 - a_1} = \frac{6-5}{4-2} = 1 \cdot 2^{-1} = 4$.
$b_1 = \frac{b_1 - b_0}{a_1 - a_0} = \frac{5-2}{2-1} = 3 \cdot 1^{-1} = 3$.
$p(x) = p(x) + b_1 \cdot q(x) = 2 + 3(x+6) = 2 + 3x + 18 = 3x + 6$.
$q(x) = q(x)(x - a_1) = (x+6)(x-2) = (x+6)(x+5) = x^2 + 4x + 2$.

		$i=0$	$i=1$				
	a_j	b_j	b_j			$p(x)$	$q(x)$
$j=0$	1	2				2	$x+6$
$j=1$	2	5	3			$3x+6$	x^2+4x+2
$j=2$	4	6	4				
$j=3$	5	5	6				

Continuamos en el bucle, ahora para $i = 2$.

$b_3 = \frac{b_3 - b_2}{a_3 - a_1} = \frac{6-4}{5-2} = 2 \cdot 3^{-1} = 3$.
$b_2 = \frac{b_2 - b_1}{a_2 - a_0} = \frac{4-3}{4-1} = 1 \cdot 3^{-1} = 5$.
$p(x) = p(x) + b_2 q(x) = 3x + 6 + 5(x^2 + 4x + 2) = 5x^2 + 23x + 16 = 5x^2 + 2x + 2$.
$q(x) = q(x)(x - a_2) = (x^2 + 4x + 2)(x - 4) = (x^2 + 4x + 2)(x + 3) = x^3 + 6$.

		$i=0$	$i=1$	$i=2$			
	a_j	b_j	b_j	b_j		$p(x)$	$q(x)$
$j=0$	1	2				2	$x+6$
$j=1$	2	5	3			$3x+6$	x^2+4x+2
$j=2$	4	6	4	5		$5x^2+2x+2$	x^3+6
$j=3$	5	5	6	3			

Por último, entramos en el bucle, con $i = 3$.

$b_3 = \frac{b_3 - b_2}{a_3 - a_0} = \frac{3-5}{5-1} = (-2) \cdot 4^{-1} = 5 \cdot 2 = 3$.

		$i=0$	$i=1$	$i=2$	$i=3$		
	a_j	b_j	b_j	b_j	b_j	$p(x)$	$q(x)$
$j=0$	1	2				2	$x+6$
$j=1$	2	5	3			$3x+6$	x^2+4x+2
$j=2$	4	6	4	5		$5x^2+2x+2$	x^3+6
$j=3$	5	5	6	3	3	$\mathbf{3x^3+5x^2+2x+6}$	x^4+2x^3+6x+5

Y tenemos al final el polinomio interpolador.

Observaciones:

1. Tal y como hemos descrito el algoritmo, al calcular el valor de una diferencia dividida borra uno que existía previamente, de tal forma que al final sólo quedarían guardados aquellos valores que se utilizan para calcular el polinomio de Newton. En el ejemplo que hemos hecho, tendríamos al final $b_0 = 2$, $b_1 = 3$, $b_2 = 5$ y $b_3 = 3$. Si quisiéramos almacenarlos todos deberíamos crear una matriz b_{ij} para las diferencias divididas.

   En la tabla, no obstante, hemos conservado todos estos valores.

2. Si hemos calculado un polinomio por este método, y nos añaden un dato nuevo, los cálculos realizados nos sirven para calcular el nuevo polinomio. Bastaría con añadir una nueva fila al final, y calcular las correspondientes diferencias divididas.

   Por ejemplo, supongamos que además de las condiciones expresadas anteriormente ($p(1) = 2, p(2) = 5, p(4) = 6$ y $p(5) = 5$) nos dicen que el polinomio debe verificar que $p(3) = 1$.

   Tendríamos entonces $a_4 = 3$ y $b_4 = 1$

		$i=0$	$i=1$	$i=2$	$i=3$			
	a_j	b_j	b_j	b_j	b_j		$p(x)$	$q(x)$
$j=0$	1	2					2	$x+6$
$j=1$	2	5	3				$3x+6$	x^2+4x+2
$j=2$	4	6	4	5			$5x^2+2x+2$	x^3+6
$j=3$	5	5	6	3	3		$3x^3+5x^2+2x+6$	x^4+2x^3+6x+5
$j=4$	3	1						

   Y ahora completaríamos la última fila:

   Para $i = 1$, $b_4 = \frac{b_4 - b_3}{a_4 - a_3} = \frac{1-5}{3-5} = (-4) \cdot (-2)^{-1} = 3 \cdot 5^{-1} = 2$.

   Para $i = 2$, $b_4 = \frac{b_4 - b_3}{a_4 - a_2} = \frac{2-6}{3-4} = (-4) \cdot (-1)^{-1} = 4 \cdot 1^{-1} = 4$.

   Para $i = 3$, $b_4 = \frac{b_4 - b_3}{a_4 - a_1} = \frac{4-3}{3-2} = 1 \cdot 1^{-1} = 1$.

   Para $i = 4$, $b_4 = \frac{b_4 - b_3}{a_4 - a_0} = \frac{1-3}{3-1} = (-2) \cdot 2^{-1} = -1 = 6$.

   Y una vez calculado esto, tendríamos:

   $p(x) = p(x) + b_4 q(x) = 3x^3 + 5x^2 + 2x + 6 + 6(x^4 + 2x^3 + 6x + 5) = 6x^4 + x^3 + 5x^2 + 3x + 1$.

   $q(x) = q(x)(x - a_4) = (x^4 + 2x^3 + 6x + 5)(x - 3) = (x^4 + 2x^3 + 6x + 5)(x + 4) = x^5 + 6x^4 + x^3 + 6x^2 + x + 6$.

		$i=0$	$i=1$	$i=2$	$i=3$	$i=4$		
	a_j	b_j	b_j	b_j	b_j	b_j	$p(x)$	$q(x)$
$j=0$	1	2					2	$x+6$
$j=1$	2	5	3				$3x+6$	x^2+4x+2
$j=2$	4	6	4	5			$5x^2+2x+2$	x^3+6
$j=3$	5	5	6	3	3		$3x^3+5x^2+2x+6$	x^4+2x^3+6x+5
$j=4$	3	1	2	4	1	6	$\mathbf{6x^4+x^3+5x^2+3x+1}$	$x^5+6x^4+x^3+6x^2+x+6$